Resolved Caveats—Cisco IOS Release 12.0(29)S1

Cisco IOS Release 12.0(29)S1 is a rebuild of Cisco IOS Release 12.0(29)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(29)S1 but may be open in previous Cisco IOS releases. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

Miscellaneous

- CSCef40187

  Symptoms: An SRP interface is stuck and there is no response at all. In the output of the **show srp topology** command, the last topology packet that is received takes more than five seconds to arrive. In addition, the “zero encap length” counter in the output of the **show hardware pxf cpu stat interface srp 1/1 detail** command increases.

  Conditions: This symptom is observed on a Cisco 10720 when the value of the overall packet size divided by 32 is 1 or 2.

  Workaround: There is no workaround.

- CSCef44154

  Symptoms: When an MPLS packet that enters through an SRP or Ethernet interface contains an L2TP or UTI packet and this MPLS packet is processed by the RP instead of the PXF engine (for example, when the IP header in the MPLS packet contain options and the MPLS TTL equals 0 or 1), the SRP or Ethernet interface stops receiving packets.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

- CSCef52419

  Symptoms: In Cisco IOS software releases earlier than Cisco IOS Release 12.0(27)S3, Release 12.0(28)S1, and Release 12.0(30)S, the CPU utilization of a Cisco 10720 is high (x%/y%, where y is greater than 60 percent), and continuous BGP and LDP flapping is reported. The counters in the output of the **show interface** command show a large number of drops and the output of the **show buffers** command shows a large number of cache misses for the private IBC buffer pools.

Conditions: This symptom is observed when the Cisco 10720 functions in a broadcast ARP storm environment and when the *length* argument of the **hold queue** *length* **in** interface configuration command is not the default of 75 packets for any interface of the router (for example, the *length* argument is 2048).

Workaround: Revert the **hold queue** *length* **in** interface configuration command and the **hold queue** *length* **out** interface configuration command to the default setting on all interfaces with non-default hold queues.

- CSCef67078

  Symptoms: A PXF buffer leak occurs on an L2TPv3 decapsulation router, which van be observed in the output of the **show hardware pxf cpu buffer** command:

```
router#show hardware pxf cpu buffer
FP buffers
pool   size    # buffer    available   allocate failures    low buffer drops
------------------------------------------------------------------------------
0      9344    1293        1293        0                    0
1      1664    12930       12930       0                    0
2      640     26746       127         0                    77165
3      256     34072       34072       0                    0
4      128     59934       59934       0                    0
```

  Depending on the packet size, the buffer leak can occur in different pools.

  Conditions: The symptom is observed on a Cisco 10720 in the following two scenarios:

  - An MPLS-enabled interface is the network backbone for L2TPv3 tunnels.
  - An 802.1q interface is the network backbone for L2TPv3 tunnels and an input security ACL with more than 400 lines is configured on the 802.1q backbone interface.

  Workaround: There is no workaround.

- CSCeg10642

  Symptoms: When six queues are configured on an interface and some of the queues do not have traffic, the bandwidth of those inactive queues should be given to other active queues (queues with traffic) in proportion to their EIR (configured via bandwidth remaining). However, this is not the case. The bandwidth is not proportionally given to all the queues.

  Conditions: Configure a policy map that creates six queues in an interface.

  Workaround: There is no workaround.

- CSCeg11421

  Symptoms: A Cisco 10720 crashes when you delete an IPv6 ACL.

  Conditions: This symptom is observed when you delete the IPv6 ACL during the TurboACL compilation.

  Workaround: Wait for the ACL to be fully compiled before you delete it.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages.
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP "source quench" messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Resolved Caveats—Cisco IOS Release 12.0(29)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(29)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdx55178

  Symptoms: Difficulties may occur when you attempt to remotely log in to a Cisco router that supports ATM. After you have established a virtual terminal connection to the system, the following user access verification sequence may be displayed, and the connection terminated:

  ```
  Password:
  Password:
  Password:
  % Bad passwords
  ```

  Conditions: This symptom is observed on a Cisco router that support ATM when an interactive ATM ping is terminated abnormally.

  Workaround: Instead of using an interactive ATM ping, enter the **ping atm interface** *atm interface vpi vci* [**seg-loopback** | **end-loopback**] [*repeat* [*timeout*]] privileged EXEC command.

- CSCea21328

  Symptoms: After a Versatile Interface Processor (VIP) has reloaded, there does not seem to be a crashinfo file because the crashinfo file is not closed; therefore, it is not visible or accessible. If the same VIP reloads again, both the first and second crashinfo files are accessible.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(6f). The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCec69536

  Symptoms: When you reload a Cisco 7500 series router with a new Cisco IOS software image, the router may reload unexpectedly during the bootup process and generate an “Imprecise cache parity error” message.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Route Switch Processor 8 (RSP8) and that runs Cisco IOS Release 12.0 S or Release 12.2(18)S when you reload the router with an image of Cisco IOS Release 12.3 T.

  Workaround: Do not reload the router. Rather, power-cycle the router to properly load the image of Cisco IOS Release 12.3 T.

- CSCed33110

  Symptoms: A VIP crash can lead to a memory exhaustion situation on the RSP in turn leading to an RSP crash.

  Conditions: This will happen more frequently on routers with a high idb count.

  Workaround: There is no workaround.

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCed75238

  Symptoms: A serial interface on a Cisco 7500 series may stop transmitting traffic and may report the following VIP crashes:

```
%MDS-2-LC_FAILED_IPC_ACK: RP failed in getting Ack for IPC message of size 84 to LC
in slot 2 with sequence 1007, error = timeout
%RSP-3-RESTART: interface Serial3/0/0:0, not transmitting
```

```
%VIP2-3-MSG: slotX VIP-3-SVIP_CYBUSERROR_INTERRUPT: A Cybus Error occurred.
%VIP2-1-MSG: slotX CYASIC Error Interrupt register 0x4000000
%VIP2-1-MSG: slotX     DMA Transmit Error
%VIP2-1-MSG: slotX CYASIC Other Interrupt register 0x100
%VIP2-1-MSG: slotX     QE HIGH Priority Interrupt
%VIP2-1-MSG: slotX     QE RX HIGH Priority Interrupt
%VIP2-1-MSG: slotX CYBUS Error Cmd/Addr 0xD00FF3A
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(5a) but may also occur in other releases. This symptom is not observed in Release 12.1(8c).

Workaround: There is no workaround.

- CSCed86286

  Symptoms: A router may reload due to a software-forced crash.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.2(13)T5 and that has SSH configured. However, the symptom may occur on other platforms that run other releases and that do not have SSH configured.

  Workaround: There is no workaround.

- CSCee16483

  Symptoms: An "RTT_FORMAT_FAIL" error may occur when the source and the target of a jitter probe do not use the same Cisco IOS release.

  Conditions: This symptom is observed when the target (or responder) runs a different Cisco IOS release than the source, and when this different Cisco IOS release on the target changes the size of the control message of the jitter, UDP, or TCP probe, causing an incompatibility between the source and the target.

  Workaround: Run the same Cisco IOS release on both the source and the target.

- CSCee35740

  Symptoms: After a VIP crashes, a FIB-3-FIBDISABLE error message due to an IPC timeout may occur for all the slots of the VIP.

  Conditions: This symptom is observed on a Cisco 7500 series after the VIP crashes and before the VIP recovers. The FIB-3-FIBDISABLE error message is generated for all the slots of the VIP, causing dCEF switching to become disabled.

  Workaround: There is no workaround. You can reenable dCEF by entering the **clear cef linecard** command.

- CSCee39972

  Symptoms: A Cisco router may experience a memory leak in the IPC buffers:

  ```
  Interface buffer pools:
  IPC buffers, 4096 bytes (total 41664, permanent 624):
       0 in free list (208 min, 2080 max allowed)
       3339198 hits, 75195 fallbacks, 0 trims, 41040 created
       4254 failures (65497 no memory)
  ```

  You can also see that the Pool Manager process is holding onto more and more memory:

  ```
  PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
     5   0  246913476   44522964  202605044  176561380    2654280 Pool Manager
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or 12.0(26)S1. The memory leak is triggered by the SNMP polling of specific OIDs within the ciscoEnhancedMemPoolMIB MIB.

  Workaround: Prevent the MIB from being polled by explicitly configuring an SNMP view in the Cisco IOS configuration. To prevent this MIB from being accessed via any community strings, create a view and apply the view to all communities configured, such as:

  ```
  snmp-server view NOMEMPOOL iso included
  snmp-server view NOMEMPOOL ciscoEnhancedMemPoolMIB excluded
  ```

```
snmp-server community public1 view NOMEMPOOL ro 6
snmp-server community public2 view NOMEMPOOL ro 7
snmp-server community public3 view NOMEMPOOL ro 8
```

The specific MIB that is being blocked is the ciscoEnhancedMemPoolMIB MIB (1.3.6.1.4.1.9.9.221).

Once the configuration is in place, the router must be reloaded to clear the IPC cache and free the memory.

- CSCee60844

  Symptoms: A software-forced crash may occur on a Cisco 7500 series.

  Conditions: This symptom is observed on a Cisco 7500 series with a PA-T3 or PA-2T3 configured for class-based weighted fair queueing (CBWFQ).

  Workaround: Remove CBWFQ from the interface or policy map.

- CSCee63808

  Symptoms: A router reloads when you enter the **show monitor event-trace merged-list** *component* command and you use a long string for the *component* argument.

  Conditions: This symptom is observed on a Cisco 7200 and Cisco 7500 series that run Cisco IOS Release 12.2 S.

  Workarounds: Enter a short string for the *component* argument.

- CSCin72727

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1. Symptom 1: The ifOperStatus SNMP object may return “Testing” when the CLI states Up/Up (Looped).

     Condition 1: This symptom is observed when PPP encapsulation and loopback are configured.

     Workaround 1: There is no workaround.

  2. Symptom 2: The ifOperStatus SNMP object may return “DOWN.”

     Condition 2: This symptom is observed when HDLC encapsulation and the **down-when-looped** command are configured.

     Workaround 2: There is no workaround.

EXEC and Configuration Parser

- CSCed51952

  Symptoms: A Cisco router may crash when you perform and online insertion removal (OIR) of a line card.

  Conditions: This symptom is observed when an interface on the line card is being configured through the CLI while the OIR of the line card removes the interface.

  Workaround: There is no workaround.

- CSCee64504

  Symptoms: A CPUHOG may occur for about 4.5 seconds when you enter the **show running-config** command.

  Conditions: This symptom is observed on a Cisco uBR10000 series but may also occur on other platforms.

Workaround: Do not enter the **show running-config** command. Rather, enter the **show config** command.

Further Problem Description: The **show tech-support** command also has a problem when it reaches the **show running-config** command part. Changing the term length does not work as workaround.

Interfaces and Bridging

- CSCed75174

  Symptoms: A router may not forward VLAN traffic.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S when there are no features configured under VLAN.

  Workaround: There is no workaround. The symptom does not occur in Release 12.0(25)S1.

- CSCee47714

  Symptoms: Entering the **shutdown** command on a controller of a Packet over T1/E1 Network Transceiver puts the controller permanently down. Entering the **no shutdown** command on the controller does not bring the controller up.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S and is specific to the controller that is installed in a PA-MC-8T1/E1, PA-MC-4T1/E1, or PA-MC-2T1/E1 port adapter.

  Workaround: There is no workaround.

- CSCee58873

  Symptoms: The **show controllers t1** *slot*/*port* command may show only the current interval.

  Conditions: This symptom is observed on a Cisco 7200 series when FDL is configured.

  Workaround: There is no workaround.

  Further Problem Description: When FDL is configured, the router updates the MIB data after checking for a valid local and remote MIB data interval that it receives from the T1 port adapter. During the remote MIB update, and if the received data interval is invalid, the router clears both the remote and the local data instead of clearing only the remote data and starting again.

- CSCin41371

  Symptoms: A Cisco 7500 series router may reload.

  Conditions: This symptom occurs on an ATM interface that flaps when there is a service policy attached to an ATM permanent virtual circuit (PVC) that has Multilink PPP (MLP) and link fragmentation and interleaving (LFI) enabled.

  Workaround: There is no workaround.

- CSCin66616

  Symptoms: The output of an snmpwalk for the entPhysicalDescr MIB on a PA-MC-8E1/120 may shows the PA-MC-8E1/120 as unknown.

  Conditions: This symptom is observed on a Cisco 7500 series in which a PA-MC-8E1/120 in installed.

  Workaround: There is no workaround.

- CSCin67296

  Symptoms: Channelized interfaces on a channelized T3 line card or port adapter that is configured for Frame Relay encapsulation may be in the up/down state, and DLCIs are inactive.

Conditions: This symptom is observed when you reload a Cisco platform and when the interfaces were in the up/up state before you reloaded the platform.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller of either the T3 line card or port adapter on the Cisco platform or on the T3 line card or port adapter on the platform at the remote end.

Alternate Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the main interface on the Cisco platform.

- CSCin74070

  Symptoms: Performance degrades when the number of VCs through which traffic is sent is scaled for PCRoMPLS AToM VCs.

  Conditions: This symptom is seen on a Cisco 7500 series with a PCRoMPLS configuration on VCs.

  Workaround: There is no workaround.

- CSCin76595

  Symptoms: A Cisco 7500 series may show a large number of tracebacks of the "64bit read" access type on a VIP.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S or Release 12.3 when the VIP contains a PA-POS-OC3, PA-POS-2OC3, or PA-SRP-OC12.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCea59206

  Symptoms: When you configure the **distribute-list** router configuration command under the **address-family ipv4 vrf** *vrf name* router configuration command, the **distribute-list** router configuration command may appear under the main routing process as may be displayed in the output of the **show running-config** EXEC command.

  Conditions: This symptom is observed in either a Routing Information Protocol version 2 (RIPv2) or a Border Gateway Protocol (BGP) configuration when you specify the *interface-type* and *interface-number* arguments of the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} [*interface-type interface-number*] router configuration command.

  The symptom does not occur when you do not define the *interface-type* and *interface-number* arguments and only enter the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} router configuration command.

  Workaround: There is no workaround.

- CSCed33044

  Symptoms: ARP may not function properly on the remote side of point-to-point Fast Ethernet link with a default static route until the remote side is pinged.

  Conditions: This symptom is observed on a Cisco router when ARP and /31 mask are configured on a point-to-point link Fast Ethernet link with a default static route. The symptom is platform-independent.

  Workaround: There are four different workarounds:

  - Use a /30 netmask on the point-to-point Fast Ethernet connection.
  - Configure a static ARP entry for the remote side of the Fast Ethernet link.

  - Enter the **ip proxy-arp** command on the remote side of the Fast Ethernet link.
  - Use an OSPF route instead of a default static route.

- CSCed57403

  Symptoms: When a Cisco router is a midpoint of a TE tunnel and the tunnel headend is a third- party vendor router, the Cisco router may crash.

  Conditions: This symptom is observed during a period of network instability and may occur when a TE tunnel does not contain an EXPLICIT ROUTE object and when the tunnel is dynamically routed by using OSPF cost only.

  Workaround: Use an EXPLICIT ROUTE object or ensure that there are no alternate paths in the network.

- CSCed59978

  Symptoms: A router may crash and reload due to a bus error, and the following error message may appear:

  ```
  Unexpected exception, CPU signal 10
  ```

  Conditions: This symptom is observed on a Cisco router that is running OSPF and that is configured for incremental SPF.

  Workaround: Remove incremental SPF from the router by entering the **router ospf** *process-id* command followed by the **no ospf** command.

- CSCed60800

  Symptoms: The withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table.

  Conditions: This symptom is observed when the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured.

  Workaround: Enter the **clear ip bgp *** or disable the **maximum-paths eibgp** command or **maximum-paths ibgp** command.

  Alternate Workaround: if the number of possible BGP paths is less or equal to 2 then the problem is transient and not obviously noticeable.

- CSCed62479

  Symptoms: The **neighbor next-hop-unchanged** command may not keep the next hop unchanged for internal paths.

  Conditions: This symptom is observed when an internal route is learnt via a confederation eBGP peer.

  Workaround: There is no workaround.

- CSCed93630

  Symptoms: A Cisco router running Cisco IOS Release 12.0 S, 12.2 S, or 12.3 T can reload unexpectedly.

  Conditions: The problem can occur only if a **bgp debug** command is enabled.

  Workaround: There is no workaround.

- CSCee10426

  Symptoms: A BGP prefix may receive or advertise incorrect label information.

  Conditions: This symptom is observed on an MPeBGP session between ASBRs when there is more than one MPeBGP session configured.

Workaround: There is no workaround.

- CSCee11274

  Symptoms: BGP may fail to reestablish a session when you remove a line card, PA, VIP, or module and replace it with a card of a different type. For example, the problem occurs when you remove a 1-port GE line card and replace it with a 3-port GE line card. However, if you replace the 1-port GE line card with another 1-port GE line card (or you just plug the same 1-port GE line card back in the chassis), the problem does not occur.

  Conditions: This symptom is observed when the router one side of the BGP session is configured with the **neighbor** *ip-address* **transport connection-mode active** command and when a line card, PA, VIP, or module is changed on the router at the other side of the BGP session. Furthermore, the router at the other side of the BGP session is configured with the **neighbor** *ip-address* **update-source** *interface* command, and the *interface* argument refers to the interface on the line card, PA, VIP, or module that is changed.

  Workaround: Disable and reenter the **neighbor** *ip-address* **update-source** command.

- CSCee24899

  Symptoms: A router that is configured for multicast routing may reload due to a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software release that contains the fix for CSCec80252. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec80252. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCee28148

  Symptoms: After a switchover on a router, one or more obsolete LSAs from a neighboring router may still be present in the topology. This is improper behavior: the LSAs should no longer be present in the topology.

  Conditions: This symptom is observed when a switchover occur on a Cisco router that runs OSPF NSF and when a neighboring router flushes one or more of its self-originated LSAs.

  Note that the LSAs automatically age out within an hour, unless the link that connects the router and the neighboring router is a demand circuit or has OSPF "flood-reduction" configured.

  Workaround: If the LSA is an external LSA (type5/type7), enter the **clear ip ospf redistribution** command on the neighboring router. In all other cases, enter the **clear ip ospf process** command on the neighboring router.

- CSCee35125

  Symptoms: A Cisco router may crash when you enter the **clear ip route *** command.

  Conditions: This symptom is observed when the routing table has a default route.

  Workaround: There is no workaround.

- CSCee36622

  Symptoms: ABRs may continue to generate summary LSA(s) for obsolete non-backbone intra-area route(s).

  Conditions: This symptom occurs under the following conditions:

  1. The ABR (call ABR X) has at least one non-backbone area (call area X) in common with one or more additional ABRs.

2. The ABRs are generating summary LSAs, on behalf of the Area X's two or more intra-area routes, into the backbone area and other areas. The two intra-area routes must be advertised as stub links from two different routers; i.e., one from ABR X, and the other from another router belonging to Area X.
3. The summary LSA IDs for the intra-area routes above, when ORed with the host bits of the corresponding masks, yield identical LSA IDs.

   For example, 10.10.10.128/25 and 10.10.10.0/24 yield identical LSA IDs when the network address is logically ORed with the host bits; i.e.,

```
10.10.10.128 | 0.0.0.127 = 10.10.10.255
10.10.10.0   | 0.0.0.255 = 10.10.10.255
```

Workaround: Perform the **clear ip ospf proc** command on all ABRs containing the obsolete LSAs.

- CSCee36721

  Symptoms: An OSPF Designated Router (DR) may fail to regenerate the network LSA when you reload the router.

  Conditions: This symptom is observed on a Cisco router that functions as a DR for an OSPF interface when another interface with the same interface address is present in the area but is in a shut down state.

  Workaround: Remove the duplicate interface address and enter the **clear ip ospf process** command.

- CSCee40207

  Symptoms: The BGP Open processes may hold more and more memory, may cause a memory leak, may finally run out of memory, and may cause a Malloc Failure error.

  Conditions: This symptom is observed when there are BGP neighbors stuck in the active state (that is, a BGP neighbor is configured but the peer address is not reachable) and when some NSF/SSO RP switchovers occur and the standby becomes active.

  Workaround: Shut down the neighbors that are not used.

  Further Problem Description: When the memory leak occurs, it will be a consistent 1k leak for each neighbor that is not up every 2 minutes.

- CSCee42285

  Symptoms: Non-EIGRP originated routes are not supported. Furthermore, when a route is injected into mp-BGP from a connected, static, or any other IGP on the remote PE router where the same prefix is also learned via EIGRP (when a backdoor exists for that site), the route may constantly flap between EIGRP and BGP.

  Conditions: These symptoms are observed when the EIGRP MPLS VPN PE-CE SoO feature is configured.

  Workaround: Only inject EIGRP routes into mp-BGP for sites with a backdoor.

- CSCee43166

  Symptoms: The BGP inbound update processing becomes slow and a high CPU utilization occurs for a long time.

  Conditions: This symptom is observed when a large number of VRFs (more than 200) and prefixes (more than 220,000) are configured.

  Workaround: There is no workaround.

- CSCee49764

  Symptoms: The **redistribute maximum-prefix** command may not take effect.

Conditions: This symptom is observed when you enter this command while OSPF is processing an SSO switchover.

Workaround: Enter the **clear ip ospf redistribution** command.

- CSCee59315

  Symptoms: A BGP VPNv4 table may contain paths that may be imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix.

```
An example of a path from a deleted BGP table entry is as follows:
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 52
Paths: (1 available, best #1, table vpn2)
  Advertised to non peer-group peers:
  10.4.1.2
  2 100, imported path from 2829:2829:185404173:11.13.11.13/-53
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:3
```

  The entry that this path is imported from has been removed from the table and its memory contents contain an incorrect pattern. When the incorrect pattern is displayed as a prefix, it appear as "2829:2829:185404173:11.13.11.13/-53".

  A mismatched prefix appears as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 54
Paths: (2 available, best #1, table vpn2)
Flag: 0x820
  Advertised to non peer-group peers:
  10.10.10.10 10.20.20.20
  2
    10.4.1.2 from 10.4.1.2 (10.4.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:2
  2 100, imported path from 200:2:172.16.0.0/24
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external
      Extended Community: RT:1:3
```

  This BGP VPNv4 table entry is for prefix 192.168.0.0/32 but it shows that a path is imported from 172.16.0.0/24. This situation occurs when a path has a link to a deleted BGP table entry, and then the memory for the deleted entry is reused for a new table entry of which the prefix may not match with the importing entry.

  Conditions: These symptoms are observed when you enter the **maximum-paths import** *number* command in router BGP address-family IPv4 VRF mode. The *number* argument indicates the number of paths to import from one VRF to another.

  Workaround: Remove the **maximum-paths import** *number* command from the router BGP address-family IPv4 VRF mode.

- CSCee63825

  Symptoms: When BGP receives an update with only a VPN label change, BGP may not update the TFIB with the new label information.

  Conditions: This symptom is observed when BGP receives an update with only a VPN label change but without any nexthop changes.

  When the symptom occurs, enter the **clear ip route vrf** *vrf-name* command to return to proper operation.

  Workaround: There is no workaround.

- CSCee65066

  Symptoms: The CISCO-PIM-MIB trap ciscoPimInvalidJoinPrune is supposed to contain the following varbinds:

  ```
  1.3.6.1.4.1.9.9.184.1.1.4 - cpimLastErrorOriginType
  1.3.6.1.4.1.9.9.184.1.1.5 - cpimLastErrorOrigin
  1.3.6.1.4.1.9.9.184.1.1.6 - cpimLastErrorGroupType
  1.3.6.1.4.1.9.9.184.1.1.7 - cpimLastErrorGroup
  1.3.6.1.4.1.9.9.184.1.1.8 - cpimLastErrorRPType
  1.3.6.1.4.1.9.9.184.1.1.9 - cpimLastErrorRP
  1.3.6.1.4.1.9.9.184.1.1.2 - cpimInvalidJoinPruneMsgsRcvd
  ```

  However, when the trap is sent, a wrong OID is used for the cpimInvalidJoinPruneMsgsRcvd.

  From a sniffer trace, the following varbind is seen: 1.3.6.1.4.1.9.9.184.2.0.5.0. The actual value sent is correct, though.

  Similarly, another CISCO-PIM-MIB trap, ciscoPimInvalidRegister, has the wrong varbind for cpimInvalidRegisterMsgsRcvd. However the value sent is correct in this case too.

  Conditions: This symptom is platform-independent and software-independent. Note that the actual value that is sent in the wrong OID for cpimInvalidJoinPruneMsgsRcvd or cpimInvalidRegisterMsgsRcvd is correct. However, this situation causes confusion on the traps receiver side because the receiver cannot decode the traps correctly.

  Workaround: There is no workaround.

- CSCee67164

  Symptoms: A router LSA is not generated for a loopback address.

  Conditions: This symptom is observed when you assign an IP address to an unnumbered interface.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the loopback interface.

- CSCee67450

  A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the **bgp log-neighbor-changes** command configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the **show ip bgp neighbors** command or running the **debug ip bgp** *neighbor* **updates** command for a configured BGP neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

- CSCee74110

  Symptoms: An RP may crash during the BGP router process after BGP flaps several times.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim Release of Release 12.0(29)S. However, this caveat is resolved in Release 12.0(29)S. This caveat is platform-independent and may occur on another platform that has an RP and that is configured for BGP.

  Workaround: There is no workaround.

- CSCee83549

  Symptoms: When multipath is configured, one of the paths may have an inconsistent (old) label, causing only one path to be operational.

  Conditions: This symptom is observed when BGP does not update the outlabel information in the TFIB and for CEF.

  Workaround: Clear or readvertise the route that is inoperational.

- CSCee89438

  Symptoms: An MSDP enabled RP does not build an (S,G) state from its SA cache when it should do so. Depending on the topology and if an SPT threshold is configured as infinite, this situation may result in a multicast forwarding interruption of up to 2 minutes.

  Conditions: This symptom is observed when the RP for a group fails and an incoming (*,G) join message is received.

  MSDP should create an (S,G) state from its SA cache. However, this is done before the (*,G) olist is populated; because of the (*,G) NULL olist, MSDP does not install an (S,G) state.

  Workaround: Enter the **clear ip mroute *** command on all first-hop routers to the source to enable the FHR to register immediately when the next packet creates an (S,G) state.

- CSCee95844

  Symptoms: BGP does not efficiently pack updates for VPNv4 prefixes; the prefixes are slowly advertised because there is only one prefix in each update.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release of Release 12.0(29)S. However, this caveat is resolved in Release 12.0(29)S.

  Workaround: There is no workaround.

- CSCef00296

  Symptoms: A router crashes when you remove the peer-group members.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: There is no workaround.

- CSCef17311

  Symptoms: An %ALIGN-3-SPURIOUS error message and a traceback may be generated when you configure BGP and MPLS VPN.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(9.10)T but may also occur in other releases such as Release 12.0 S and Release 12.2 S.

  Workaround: There is no workaround

- CSCin65241

  Symptoms: ISIS redistribute commands are not synced to the standby RP. The routes dependent on these commands will fail after switchover.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

ISO CLNS

- CSCee54672

  Symptoms: The redistribution of routes from L1 into L2 or/and from L2 into L1 may not occur properly, and a learned IS-IS prefix may be missing.

  Conditions: This symptom is observed under the following conditions:

  – There are multiple paths to reach the same prefixes.

  – One source LSP removes a prefix and another LSP adds the same prefix, while both paths between the prefix and the LSPs are of equal cost.

  Workaround: Enter the **clear isis *** or the **clear ip route *** command to restore the prefix. However, doing so clears all the routes and recalculates them again, which is a disruptive action.

Miscellaneous

- CSCdx59158

  Symptoms: An active Route Processor (RP) sets the link correctly to the “down” state, but the standby RP fails to set the link correctly.

  Conditions: This symptom is observed on a Cisco 10000 series when the far end causes the link state to flap from “up” to “down.” However, the symptom is not platform-specific and may also occur on other platforms that have dual RPs.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCdx87477

  Symptoms: The adjacency table does not display information that is related to the virtual access interface of a network access server (NAS) when the **show adjacency detail** EXEC command is entered.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(13)T or Release 12.2(14)S but may also occur in other releases.

  Workaround: There is no workaround.

- CSCdz56772

  Symptoms: A router that is configured for Cisco Express Forwarding version 6 (CEFv6) may reload when the supported state of an interface changes and when the associated prefix is deleted.

  For example, a router may reload when a tunnel interface changes from a CEFv6 unsupported mode (for example, generic route encapsulation [GRE] IP version 6 [IPv6]) to a supported mode (for example, IPv6 IP) and you remove the associated IPv6 address by entering the **no ipv6 address** *ipv6-address* interface configuration command or by shutting down the tunnel interface.

  Conditions: This symptom is observed on all platforms that run Cisco IOS Release 12.2 S or Release 12.2(13)T but may also occur in other releases.

Workaround: There is no workaround.

- CSCea28043

  Symptoms: IP commands that are sent in the Cisco Networking Services (CNS) config-changed event output may contain an extra **ip** prefix.

  Conditions: This symptom is observed on a Cisco router when you enter both **ip** global configuration commands and the **cns config notify** *diff* global configuration command to capture commands that change configuration for the config-changed event output.

  Workaround: Enter the *all* keyword in the **cns config notify** global configuration command. This workaround is not valid when the only changes in the configuration occur in the config-changed event output.

- CSCea29640

  Symptoms: A 1-port High-Speed Serial Interface network module (NM-1HSSI) that is running Frame Relay traffic shaping (FRTS) and Frame Relay fragmentation 12 (FRF.12) may randomly stop functioning and does not recover on its own. This problem is not limited to FRF.12 and could also occur with other configurations.

  Conditions: This symptom is observed on a Cisco 3600 router that is running Cisco IOS Release 12.2(11)T1 or Release 12.2(13a) but may also occur in other releases. In addition, the symptom may also occur on a Cisco 7200 series.

  Workaround: Disabling FRF.12 fragmentation might help.

  First Alternate Workaround: Enter the **clear interface** EXEC command on the affected interface.

  Second Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCea57710

  Symptoms: A Cisco router may log the following traceback error:

  ```
  %ATMPA-3-BADPARTICLE: Switch1: bad rx particle 0x61CA8040 flags 0x00000001 index 9937
  Traceback= 6007968C 6008F404 60E844F0 60E815F4 60D80BF4 60D8E8A4 6009CF94 600B56EC
  ```

  Conditions: This symptom occurs in the following configuration:

  - A total of 1000 Virtual Private Network (VPN) routing/forwarding (VRF) interfaces are enabled on each RPM-PR.
  - About 98,000 VPN routes have permanent virtual circuits (PVCs).
  - Cell-based Multiprotocol Label Switching (MPLS) is configured for Label Switch Controller (LSC) hot redundancy.
  - Each RPM-PR has 500 external Border Gateway Protocol (EBGP) sessions.
  - The VPN prefixes are advertised with /24(90%) and /30(10%) subnets.

  Workaround: There is no workaround.

- CSCeb52330

  This caveat consists of two symptoms, two conditions, and two workarounds.

  1. Symptom 1: The interface commands in the CNS configuration notify changed message contain unexpected data.

     Condition 1: This symptom is observed when you configure the CNS **cns config notify** *diff* global configuration command and you configure **interface** global configuration commands on the Cisco IOS device.

Workaround 1: There is no workaround if only the changes in the configuration are expected in the CNS configuration notify changed message.

Alternate Workaround 1: Specify the *all* option for the cns config notify global configuration command.

2. Symptom 2: Once the **cns config notify** global configuration command is configured, the router may not detect a newly created interface.

   Condition 2: This symptom is observed when the *diff* option in the **cns config notify** global configuration command is selected and a new dynamic interface is created.

   Workaround 2: There is no workaround.

- CSCed24020

  Symptoms: The IP multicast throughput in Cisco IOS Release 12.3(6)T is not as good as in Release 12.3(4)T.

  Conditions: This symptom is observed when more than 130 kpps of traffic is sent. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed35964

  Symptoms: Interoperating problems may occur with a particular third-party vendor 48 MB flash card, and a router may not be able to read the flash card with “bad majic” and “-13 open file” error messages.

  Conditions: This symptom is observed in the following two scenarios:

  – Scenario 1: If the flash card is formatted on one router and then inserted in another router, the boot image and Cisco IOS image can be read from the flash card until you reload the router. After the router is reloaded, “bad majic” and “-13 open file” error messages occur.

  – Scenario 2: When you remove the first large file from the flash card (irrespective of its position on the flash card and irrespective of whether or not the file is a Cisco IOS file) and you reload the router, “bad majic” and “- 13 open file” error messages occur, and the router may enter a continuous loop. The symptom occurs with the removal of a file that is 12 MB or 14 MB but does not occur with the removal of a file of 4 MB.

  Workaround: There is no workaround.

- CSCed55962

  Symptoms: From a local customer edge (CE) router, you may not be able to reach or ping some prefixes (subnets) on a remote CE router over an Multiprotocol Label Switching (MPLS) network.

  Conditions: This symptom is observed in a cell-based MPLS network.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected subinterface that is connected to the local CE router. Doing so enables the Border Gateway Protocol (BGP) to run a scan again and repopulates the subnets in the Tag Forwarding Information Base (TFIB).

- CSCed57925

  Symptoms: The cisco.mgmt.cns.config-changed event message is not generated when **atm pvc** CLIs are configured.

  Conditions: This may occur when the CNS configuration notify agent is configured by the **cns config notify** command and **atm pvc** CLIs are configured.

  Workaround: There is no workaround.

- CSCed63357

  This caveat consists, of six separate symptoms, conditions, and workaround, of which the first three apply to all Cisco IOS releases and the last three apply only to Cisco IOS Release 12.3 T:

  1) Symptoms: There are three symptoms:

  - There may be a inconsistent or duplicate display of files between the **show disk***slot-number* and **dir disk***slot-number* commands.
  - When a file is deleted from the CLI, the file may be deleted but a "No such file" message may be printed.
  - One cluster may leak. Entering the **fsck** command truncates the original file and creates an orphan file for the leaked cluster.

  Conditions: This symptom is observed when an application creates or opens a file without the "O_TRUNC:" mode, as in the following example:

```
show version | append disk#:

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#vtp file new
Setting device to store VLAN database at filename new.
Router(config)#^Z
```

  Workaround: There is no workaround.

  2) Symptoms: The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information (such as inconsistent file sizes) when multiple images are copied.

  Conditions: This symptom is observed when you make two copies of the image file to the disk by using two vtys and by entering the **dir disk***slot-number* command at the same time.

  Workaround: Do not enter the **show disk***slot-number* and **dir disk***slot-number* commands when multiple images are being copied.

  3) Symptoms: There are two symptoms:

  - The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
  - Entering the **fsck** command may delete or truncate the valid files or create an orphan file for an unused cluster.

  Conditions: This symptom is observed when you rename a directory that consists of many subdirectories or files.

  Workaround: Reload the router.

  4) Symptoms: There are two symptoms:

  - There may be a duplicate entry for each file when you enter the **show disk***slot-number* command.
  - An snmpGet on a ciscoFlashFileSize object may enter a loop.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T after the router boots up.

  Workaround: There is no workaround.

  5) Symptoms: There are two symptoms:

  - The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
  - Entering the **fsck** command may delete or truncate the original file.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T when an application or a CLI command overwrites a file on the disk.

Workaround: Reload the router.

6) Symptoms: A router that runs Cisco IOS Release 12.3 T crashes.

Conditions: This symptom is observed when an application creates or opens a file without the "O_TRUNC" mode and attempts to delete the file, as in the following example:

```
show version | append disk0:redirect.out" and issuing
delete disk0:disk0:redirect.out
```

Workaround: Reload the router and delete the file.

- CSCed67734

  Symptoms: Packet processing at the remote end of a link may fail.

  Conditions: This symptom is observed when a service policy that includes the **set atm-clp** command is enabled on an output interface via the **service-policy output** command; the platform that links to this output interface at the remote end drops the packets.

  Workaround: Remove the **set atm-clp** command from the service policy on the output interface.

- CSCed70198

  Symptoms: The line protocol may go down.

  Conditions: This symptom is observed when Frame Relay fragmentation is enabled on the main interface.

  Workaround: There is no workaround.

- CSCed75108

  Symptoms: When an IP VRF is configured on an SDCC interface of a Cisco 10720 router, all MPLS packets which are to be forwarded through the SDCC interface are instead dropped by the PXF forwarding engine.

  Conditions: This problem is observed when setting up an MPLS-VPN in which the PE-CE interface is an SDCC interface on the Cisco 10720 router.

  Workaround: Disable the PXF forwarding path via the **no service pxf** command.

  Further Problem Description: The forwarding path must deal with MPLS packets that are destined for the SDCC interface by punting them rather than dropping them.

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

  Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

  Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- CSCed78519

  Symptoms: SCR continues to filter CLP(0) cells and tag CLP(1) cells when the CLP(0) filter is removed from the **class-map** command.

  Conditions: This symptom is observed when there are multiple PVCs and when the class map filters are globally removed.

Workaround: There is no workaround.

- CSCed79634

  Symptoms: The percent-to-bps conversion for the **police cir percent** command that is configured in a second- and third-level policy may not function properly.

  Conditions: This symptom is observed when the **police cir percent** command is used in a two- or three-level hierarchical policy with a 1-rate 2-color policer at the higher levels (the exceed action is "not drop"); the police percent-to-bps conversions at the second and third level should be based on the interface bandwidth and not on the parent police rates, but this behavior does not occur.

  Workaround: Use a **police** command with an actual-rate configuration instead of a percent configuration.

- CSCed85254

  Symptoms: MPLS forwarding may stop.

  Conditions: This symptom is observed under the following conditions:

  - When you change a COS map or prefix map.
  - When you change an IP access list.

  Workaround: There is no workaround.

- CSCed85324

  Symptoms: Stale MPLS COS per-route entries may be left behind.

  Conditions: This symptom is observed after the route disappears from the routing table in cell mode multi-VC network.

  Workaround: There is no workaround.

- CSCed86984

  Symptoms: CEF may become disabled on a VIP, port adapter, module, or line card because of a fatal error, and the following error message may be generated:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 2: Window did not open, LC to RP IPC is
  non-operational
  ```

  Conditions: This symptom is observed after an RPR+ switchover.

  Workaround: There is no workaround.

- CSCed88286

  Symptoms: Layer 3 connectivity may be lost after toggling CEF on a provider Edge router.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2 S in an ATM/Ethernet VLAN L2 interworking configuration.

  Workaround: There is no workaround.

- CSCed92704

  Symptoms: An ATM PVC may go down when an **oam-pvc manage** command is configured.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S or a later release and that functions as a customer edge (CE) router when AIS cells are received from the provider edge (PE) router. However, the symptom is platform-independent and may also occur on other platforms.

  Workaround: Rebind the session on the PE router to enable the ATM PVC on the CE router to come up again.

- CSCed92837

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the standby Route Switch Processor (RSP) my hang just before downloading the image. This situation may prevent the router from entering the STANDBY-HOT state and from being capable to perform a switchover until the standby RSP is reset.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0 S or 12.2 S and that is configured for SSO/Nonstop Forwarding (NSF).

  Workaround: There is no workaround. After the problem occurs, you can recover the router by either waiting for an IPC timer to expire (the default time is 30 minutes) or by entering the **hw-module sec-cpu reset** command.

- CSCed93593

  Symptoms: The cisco.mgmt.cns.config-changed event message contains invalid changeItem information.

```
Example: for:  (config)#policy-map TEST2
               (config-pmap)#class m_new
               (config-pmap-c)#shape peak 8010
               (config-pmap-c)#priority
               (config-pmap-c)#exit
               (config-pmap)#desc TESTTEST
               (config-pmap)#exit
The 4th changeItem is: Context:    <empty>
                       EnteredCmd: exit
                       NewConfig#: <empty>
                       OldConfig#:
                                   !
                                   MyPolicy
                                   test
                                   TEST2
                                   description TESTTEST
                                   class m_new
                                   shape peak 8010
                                   priority
```

  The above-mentioned changeItem information is incorrect.

  Conditions: This may occur when the CNS configuration notify agent is configured by the **cns config notify** command and a policy-map CLI is configured on the Cisco IOS device.

  Workaround: There is no workaround.

- CSCee00661

  Symptoms: Changing any IP access control list (ACL) may cause a walk of all LC-ATM prefixes.

  Conditions: This symptom is observed on a router configured with an LC-ATM Multi-VC when the changed ACL is not related to the Multi-VC.

  Workaround: There is no workaround.

- CSCee01931

  Symptoms: A router may crash when you enter the **fair-queue** command on the interface of a PA-MC-STM-1 port adapter.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S when the interface has the **rate-limit output** command enabled.

Workaround: There is no workaround.

- CSCee06228

  Symptoms: The SRP protocol on a Cisco uBR7246VXR may not fully initialize during the boot sequence.

  Conditions: This symptom is observed on a Cisco uBR7246VXR running Cisco IOS Release 12.2(15)BC1b when one SRP side is wrapped. The symptom may also occur on a Cisco 7200 series and is not release-specific.

  Workaround: Force a wrap by entering the **srp ips request forced-switch** command and remove this forced wrap. Note that you have to do this manually after a reload/reboot.

- CSCee06794

  Symptoms: DTS may not work properly on dot1q Fast Ethernet subinterfaces. Traffic is not shaped at the expected rate

  Conditions: This problem is observed on a Cisco 7500 series that is configured as a PE router and that runs Cisco IOS Release 12.2(12i). The symptom may also occur in other releases.

  Workaround: If this is an option, use ISL subinterfaces.

- CSCee07351

  Symptoms: LC-ATM-enabled subinterface on a PE router stays in “not ready” state when viewing the LDP session to the LSC using the **show mpls ldp discovery** command. The **shutdown** interface command followed by the **no shutdown** interface command will not clear the problem when performed on either the LC-ATM subinterface on the PE or the Xtag interface on the connected LSC.

  Conditions: The interface stays in “interface not LDP ready” state when there exists a stray LVC on the switch interface. The PE reaches this state after multiple LDP flaps.

  Workaround: The condition may be cleared by entering the **clear ip route** *prefix* command where *prefix* is the local loopback address for the LC- ATM subinterface. This will cause all tailend LVCs on all LC-ATM subinterfaces to be torn down and re-established, causing a brief customer outage. This workaround should only be used if no alternate path exists for MPLS traffic towards this device (i.e., a redundant LC-ATM subinterface). After using this workaround, user should confirm that the expected number of LVCs has been re- established with the output of the **show mpls atm summary** command. If bindings are not successfully re-established, repeat the **clear ip route** *prefix* command, or reload the router.

  Reload of the router will remove the stray LVC and bring the LDP session on the PE’s LC-ATM subinterface back to normal state.

- CSCee09533

  Symptoms: Flapping an interface may cause a router that is configured for L2TPv3 to crash.

  Conditions: This symptom is observed on a Cisco router that has many L2TPv3 sessions and tunnels configured. For example, the symptom occurs with 2000 sessions over 2000 tunnels but also with 4000 sessions over one tunnel.

  Workaround: There is no workaround.

- CSCee12235

  Symptoms: A Cisco platform reloads because of a watchdog timer expiration.

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(20)S2 or Release 12.3 under the following conditions:

- A service policy (“A”) is attached to an ATM PVC.
- Policy-map “A” is renamed to “B”.
- Service policy “B” is attached to the ATM PVC.

Workaround: First detach the service policy from the PVC, then rename it and attach it again.

- CSCee12772

  Symptoms: On certain platforms (in particular but not limited to a Cisco 800 series), the CNS agents code that captures output for later transmission can crash.

  Conditions: This symptom is observed on a router that has configuration and EXEC agents and CNS agents that execute CLI commands when you send an XML file to direct these agents to execute a CLI command and return the output (if there is any output).

  Workaround: Telnet into the router (not through the console) and exit. This may need to be done multiple times.

- CSCee13932

  Symptoms: Cisco target FEC stack TLVs may not interoperate with those of third-party vendors.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(27)S or Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCee15581

  Symptoms: A router that is configured for L2VPN may crash.

  Conditions: This symptom is observed when L2VPN connections are dynamically deconfigured and then reconfigured.

  Workaround: There is no workaround.

- CSCee15971

  Symptoms: When the pseudo wire goes down and then comes back up, an AAL5 AToM VC with OAM emulation stays down.

  Conditions: This symptom is observed when the PVC is managed with zero as the loopback frequency. Also, when the pseudo wire goes down it moves to the AIS state, and when the pseudo wire comes back up, the VC stays in the down state. Since the loopback frequency is zero, no loopback cells are sent.

  Workaround: Delete the AAL5 VC and readd it with the same configuration.

- CSCee16581

  Symptoms: Traffic is sent using the “net ctrl” queue on the egress interface.

  Conditions: This problem occurs on a Cisco 10720 router when IPv6 high-priority traffic (110 or 111 in the first 3 bits of the IPv6 traffic class) is forwarded.

  Workaround: There is no workaround.

- CSCee19222

  Symptoms: An MLP bundle configured between a Cisco 7500 series and any other router may not be able to switch traffic when dCEF is enabled on the Cisco 7500 series.

  Conditions: This symptom is observed when LFI is enabled with one member link in the MLP bundle.

Workaround: Either remove dCEF or remove LFI. (A combination of CEF and MLP is not supported.) Note that if there are two member links in the interleaving-enabled MLP bundle, the problem does not occur.

- CSCee22045

  Symptoms: A “MSC200_MP-4-PAUSE” traceback may occur in large Frame Relay FRF.12 configurations.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series, Cisco 7500 series, and Cisco 7600 series.

  Workaround: There is no workaround. However, this message does not affect the proper operation of the router.

- CSCee23607

  Symptoms: An L2tpv3 tunnel does not come up.

  Conditions: This problem can be seen in an ATM-FR interworking scenario.

  Workaround: There is no workaround.

- CSCee23750

  Symptoms: When you enter the **format flash:** command on a router to format a LEFS flash card, the router fails to give the DOS format and displays this error:

  ```
  %Error formatting flash (Invalid DOS media or no media in slot)
  ```

  The flash card is no longer accessible until the router is reloaded.

  Conditions: This symptom is observed on any Cisco router that supports a disk file system and that runs Cisco IOS Release 12.3(6) or a later release. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee24349

  Symptoms: A Cisco 7500 series cannot boot when there are more than 256 different policy maps attached as service policies on the router.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1.

  Workaround: Do not use more than 256 service policies.

- CSCee27276

  Symptoms: A router shows a constant increase in the holding memory for the L2TP Daemon process.

  Conditions: This symptom is observed when invalid L2PTv3 control packets are sent from a peer router. Invalid packets means packets without all the mandatory attribute value pairs.

  Workaround: There is no workaround.

- CSCee30116

  Symptoms: CNS config notify events may stop coming.

  Conditions: This symptom is observed when the **cns config notify diff** command is enabled and when other CNS configuration agents are configured.

  Workaround: Enter the **no cns config notify** command followed by the **cns config notify diff** command.

- CSCee30696

  Symptoms: A VIP in a Cisco 7500 series may crash intermittently.

Conditions: This symptom is observed during AToM HDLC/PPP regression tests.

Workaround: There is no workaround.

- CSCee31618

  Symptoms: Buffer leakage could occur when a high load of traffic is sent to an interface that has a service policy enabled. This could result in ping failures or very long packet delay.

  Conditions: The problem is observed with an MC-T3+ interface that is configured in unchannelized mode, and the traffic consists only of small packets such a 64-byte packets.

  Workaround: Manually configure the **tx-ring-limit** command to lower the number of packets that can be placed on the transmission ring.

- CSCee34076

  Symptoms: Routes that are removed soon after an SSO switchover occurs may remain in the CEF table.

  Conditions: This symptom is observed when VRFs are configured.

  Workaround: There is no workaround.

- CSCee34094

  Symptoms: A standby RP keeps crashing.

  Conditions: This symptom is observed when both the **snmp-server community** *string* **rw** command and the **snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart** command are configured.

  Workaround: Remove the **snmp-server community** *string* **rw** command from the startup configuration before rebooting the router. When the router has booted, reenter the **snmp-server community** *string* **rw** command.

- CSCee35185

  Symptoms: After reloading a Cisco platform, one of the RPs may reload, or the following error message may be displayed:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```

  Conditions: This symptom may be observed on any Cisco platform that is configured with dual RPs and that supports RPR+.

  Workaround: There is no workaround.

- CSCee35331

  Symptoms: A router may reload if removing the L2TP class is followed by removing the pseudowire class.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.0(28)S when both removals are done in a very short time via an auto test script and when the L2TP sessions are already established. This is a timing related issue.

  Workaround: Wait at least 1 second before you remove the pseudowire class.

- CSCee35349

  Symptoms: When you set up an L2TPv3 tunnel configured in the PW class, a ping cannot go through from CE router 1 to CE router 2 until the ping is initiated by CE router 2.

  Conditions: This failure occurs in Cisco IOS Release 12.0(28)S with a Fast Ethernet interface (not with a serial or POS interface).

Workaround: First, ping from CE router 2 to CE router 1. Then, ping from CE router 1 to CE router 2.

- CSCee36050

  Symptoms: A VIP crashes with the following error message:

  ```
  VIP-3-SYSTEM_EXCEPTION: VIP System Exception occurred sig=10, code=0x10
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when you re-use a channel group (or subinterface) that was previously configured with a Frame Relay DLCI "set" service policy.

  Workaround: Remove the "set" service-policy before you remove the channel group (or subinterface).

- CSCee36891

  Symptoms: The PVC bundles VC selection does not work correctly.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series.

  Workaround: There is no workaround.

- CSCee38324

  Symptoms: A VIP may crash.

  Conditions: This symptom is observed on a Cisco 7500 series when QoS is configured on the interface of the VIP and traffic is flowing.

  Workaround: There is no workaround.

- CSCee38942

  Symptoms: EoMPLS tunnels do not have labels assigned to them, preventing a virtual circuit from coming up.

  Conditions: This symptom is observed when multiple (for example, 1200) EoMPLS tunnels are configured. Only on a few tunnels the symptom may not occur.

  Workaround: There is no workaround.

- CSCee38977

  Symptoms: When you flap an interface that is attached to an L2TPv3 tunnel, the tunnel may enter the shut mode.

  Conditions: This symptom is observed on a Cisco 10720 when the **xconnect** command is enabled on the interface and when you enter the **shutdown** command followed by the **no shutdown** command on the interface or when you cause the interface line protocol to go down and up again.

  Workaround: Disable and reenter the **xconnect** command on the interface.

- CSCee39853

  Symptoms: A Cisco router that is running Cisco IOS Release 12.0(25)SX1 may experience CEF disabling on standby PRE.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(25)SX1. The symptom may also occur in Release 12.0 S.

  Workaround: Reset standby PRE.

- CSCee41544

  Symptoms: If there is sequence number enabled on a PVC and you add a service policy to this PVC, the sequence number configuration is lost.

  Conditions: This symptom is observed when you enable the sequence number configuration and then add a service policy to the same PVC.

Workaround: After the symptom has occurred, readd the sequence number configuration to the PVC.

- CSCee43569

  Symptoms: The TE DB on a tunnel headend may become corrupted.

  Conditions: This symptom is observed on a Cisco router that has MPLS configured.

  Workaround: There is no workaround.

- CSCee43855

  Symptoms: Starting with Cisco IOS Release 12.0(26)S, the Cisco 10720 router supports the IPv6 ACL feature. The IPv6 packets are corrupted (including the IPv6 header) for the following scenario: For a packet in 6PE decapsulation case (MPLS to IPv6), if output ACLs are applied at the output interface and these ACLs are long enough to require a second PXF pass (known as output ACL split case), then the outgoing IPv6 packet is corrupted.

  Conditions: This symptom is observed on Cisco 10720 routers that are running Cisco IOS Release 12.0(26)S or later releases.

  Workaround: There is no workaround.

- CSCee47026

  Symptoms: The ATM HA process may crash.

  Conditions: This symptom is observed on a Cisco router that has VCS configured with local switching.

  Workaround: There is no workaround.

- CSCee52752

  Symptoms: A Cisco router may crash when interfaces are brought up or when interfaces are deleted.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S. However, this caveat is platform-independent.

  Workaround: There is no workaround.

- CSCee55068

  Symptoms: On a Cisco router that has L2 PVCs in the AIS alarm state, in addition to sending AIS cells, the router also sends loopback cells to the customer edge router.

  Condition This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S when the **oam-pvc manage** command is configured and when the L2 PVC gets enters the AIS alarm state. However, this caveat is platform-independent.

  Workaround: There is no workaround.

- CSCee56225

  Symptoms: A Cisco router may experience alignment errors involving MPLS and BGP, and the output of the **show alignment** command may show the following information:

  ```
  Total Spurious Accesses 1, Recorded 1
   Address  Count  Traceback
         C      1  0x612EE93C 0x60BD2894 0x60BD2F0C 0x60B8C2DC
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS and BGP.

  Workaround: There is no workaround. However, note that the symptoms are of a transient nature and do not affect the functionality of the router.

- CSCee58083

  Symptoms: A Cisco router that runs a Cisco IOS interim release for Cisco 12.0(29)S or interim Release 12.3(9.3) or 12.3(9.2)T may log the following error message and traceback, and IPC services using large RPC messages/replies may fail:

  ```
  %IPC-SP-5-INVALID: Invalid dest port=0x2220000
  -Traceback= 402F3784 403027CC 403025AC 4030A10C 4030A4F8 4030A7B8 402F7E78 402F8244
  40309478 402F8890 4033A0E8 40344284
  ```

  Conditions: This symptom is observed without any external trigger occurring.

  Workaround: There is no workaround.

- CSCee59585

  Symptoms: On a Cisco router, the output of the **execute-on slot** *number* **show ip cef** *prefix* command may display the same imposed label twice for a recursive public route.

  Conditions: This symptom is observed on a Cisco platform that supports distributed forwarding such as a Cisco 7500 series or a Cisco 12000 series when the **neighbor** *name* **send-label** command is configured under an IPv4 BGP address family on a VIP or line card and when one of the following actions occurs:

  - You enter the **clear cef linecard** command.
  - You perform an OIR of the VIP or line card.
  - You enter the **no ip cef distributed** command followed by the **ip cef distributed** command.

  The symptom disappears after the affected prefix flaps.

  Workaround: There is no non-impacting workaround, but you can enter the **clear ip route** *prefix* command or reset the BGP peer to solve the problem.

- CSCee66206

  Symptoms: When you boot a Cisco 7200 series that is configured with an NPE-300 or NPE-400 and that runs a c7200-js-mz image, the router may crash with a traceback.

  Conditions: This symptom is observed when the c7200-kboot-mz image is the bootloader and when the router runs Cisco IOS interim Release 12.1(22.3)E1. The symptom may also occur in other releases such as 12.0 S, 12.2 S, and 12.3.

  Workaround: There is no workaround.

- CSCee69861

  Symptoms: When a host sends a path MTU discovery packet into a L2TPv3 tunnel, a Cisco 10720 returns an ICMP unreachable packet, indicating that the path MTU is “MTU-32byte (L2TPv3 header)-(layer2 header of customer packets),” which is incorrect. This situation causes TCP communications such as FTP or HTTP downloads over the L2TPv3 tunnel to fail. For example, 26 bytes (outer IP + L2TPv3 header sizes) may be missing.

  Conditions: This symptom is observed on a Cisco 10720 that functions as a PE router.

  Workaround: If this is an option, set an MTU with a small size at the server side. If this is not an option, there is no workaround.

- CSCee69887

  Symptoms: A dual SRP ring fails to become active completely due to an is-type mismatch. The output of the **show clns neighbors** command indicates that a certain system interface remains in the “Init” state indefinitely, although the output of the **show ip interface brief** command shows that this interface is up.

Conditions: This symptom is observed when a dual SRP ring is configured on three routers that run Cisco IOS Release 12.2S. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCee70024

  Symptoms: LSP-Ping packets may include a Vendor Enterprise Code TLV Type 5 with a length that is greater than 4 and with Vendor Private Extensions. According to the draft-ietf-mpls-lsp-ping-05.txt IETF draft, the Vendor Enterprise Code TLV Length should always be 4, and the vendor extensions should use a TLV Type that is in the range 64512-65535.

  Conditions: This symptom is observed on a Cisco platform that functions in an MPLS OAM environment.

  Workaround: There is no workaround.

- CSCee71793

  Symptoms: Malformed MPLS echo request packets may cause excessive Route Processor (RP) CPU cycles to be consumed during parsing of malformed TLVs.

  Conditions: This symptom is observed when MPLS echo request packet are decoded and incorrectly parse beyond the packet boundary due to improper bounds checking.

  Workaround: There is no workaround.

- CSCee72353

  Symptoms: An LDP session over a tunnel interface may drop and not come back up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S when auto-tunnel traffic engineering is configured and when RSVP label distribution and LDP are configured in the MPLS core.

  If the **no mpls ip** command is configured on the physical interface to disable LDP, and RSVP label distribution remains enabled, auto-tunnel traffic engineering fails and you cannot bring the tunnel back up.

  Workaround: Run LDP in the MPLS core for all interfaces that have auto-tunnel traffic engineering configured.

- CSCee74886

  Symptoms: After you enter the **microcode reload pxf** command or after a PXF crash occurs, EoMPLS packets that should be encapsulated with EoMPLS encapsulation are treated as if they are normal IP packets, and are likely to be dropped by the router.

  Conditions: This symptom is observed on a Cisco 10720 router when an SRP (sub)interface is used as the EoMPLS backbone interface to transport EoMPLS packets to other EoMPLS PE routers and when the (sub)interface has the **xconnect** *destination-address vc-id* **encapsulation mpls** command enabled.

  Workaround: Remove the **xconnect** *destination-address vc-id* **encapsulation mpls** command from the (sub)interface that connects to a customer device, and reconfigure it on the (sub)interface.

- CSCee74920

  Symptoms: An RP crashes after you remove the event manager applet.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(26)S or a later 12.0 S release when an EEM policy is removed from the configuration by entering the **no event manager applet** *applet-name* command while actions within the EEM policy are being executed.

  Workaround: There is no workaround.

- CSCee76167

  Symptoms: Several spurious memory accesses occur with ATM PVCs, and an error message and traceback similar to the following one may be generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x601B5190 reading 0x74
  %ALIGN-3-TRACE: -Traceback= 601B5190 601B7B20 601B69D4 60176F64 6017776C 6017755C
  6055508C 60555EA0
  ```

  Conditions: This symptom is observed when you create ATM PVCs or when you enter the **clear interface atm** or **show atm vc** command.

  Workaround: There is no workaround.

- CSCee76306

  Symptoms: A Cisco router crashes during a period of high routing protocol activity.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(21)SP or a later release or Release 12.0(22)S or a later release.

  The crash is most likely to occur when the router holds a large number of IPv4 prefixes in its routing table and when there is a lot of turnover in the routing table, that is, prefixes are added and deleted on a rapid basis.

  Workaround: There is no workaround.

- CSCee77328

  Symptoms: The PXF forwarding engine on a Cisco 10720 may crash after the microcode is reloaded either through a manual reload by entering the **microcode reload pxf** command or after a previous PXF crash. This situation causes multiple PXF crashes.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(26)S or a later 12.0 S release, all of which contain IPv6 PXF packet forwarding functionality, and is most likely to occur while IPv6 packets are passing through the router.

  Workaround: Disable IPv6 functionality or disable PXF by entering the **no service pxf** command.

- CSCee95978

  Symptoms: A Cisco 7200 series with an NPE-G1 may crash when you ping 50 5200-byte packets from one router that functions as a generator via the Cisco 7200 series with the NPE-G1 to another router that functions as a reflector. The three routers are connected back-to-back via static routers.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(9a) but may also occur in other releases.

  Workaround: There is no workaround.

- CSCee96231

  Symptoms: A Channel Interface Processor (CIP2) and an xCPA port adapter fail to load their microcode. The microcode bundle is expanding such that the files do not have the prefix. For example, the file cip28-17_kernel_hw4 is _kernel_hw4.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7500 series. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee13801. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCef20996

  Symptoms: An SNMP query on cbQosREDClassCfg objects may take up a very large part of the CPU utilization of a router. Depending on the overall CPU utilization and query frequency, some side effects such as CPU hogs may occur.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S.

  Workaround: There is no workaround.

- CSCef21262

  Symptoms: An MPLS static label that is configured as an outgoing label is not installed in the MPLS forwarding table.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(29)S when a static label is assigned as an outgoing label for a FEC by entering the **mpls static binding ipv4** *prefix mask* **output** *nexthop label* command. The statically configured outgoing label is not installed in the MPLS forwarding table.

  Note that a static label that is assigned as a local label is properly installed in the MPLS forwarding table.

  Workaround: Configure an LDP session to the next hop router over the next hop interface, and configure the next hop router to prevent it from advertising the label for the impacted prefix by entering the **mpls ldp advertise-labels** command.

- CSCef24642

  Symptoms: The PXF engine on a Cisco 10720 may crash, and the following error messages are generated in the logging buffer (the PXF crashinfo files can be found in the flash memory of the router):

  ```
  MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
  ```

  In addition, there are four ways to verify that the symptom is occurring:

  – If the **debug main error**, **debug uplink error**, and **debug access error** commands are enabled on the router, the following error messages are also generated in logging buffer:

    ```
    MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error SRP_TX_VA_SC_GIANT_PKT
    (code 4)
    MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error
    SRP_TX_VA_SC_FIFO_GIANT_PKT(code 100)
    MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error
    VA_SC_IPM_RD_ACC_TIMER_EXP(code 1)
    MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error
    VA_RP_IPM_RD_ACC_TIMER_EXP(code 4)
    MSD: %Camr_VA-3-SISTATUS: Van Allen SRIC Data integrity error
    VA_SI_FL_CTRL_DRVN(code 80)
    MSD: %Camr_VA-3-SOSTATUS: Van Allen SROC Data integrity error VA_SO_PKT_LEN_ERR
    (code 1)
    MSD: %Camr_VA-3-STATISTICS: VA statistics register: 0x0098 reports
    VA_SO_PKT_LEN_ERR_COUNT =  3
    ```

  – In the output of the **show interface srp 1/1** command, the received error counters such as “framer runts” and “input errors” have a large value.

  - In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the "destination unreachable" counter increases.
  - In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the "zero encap length" counter increases.

  Conditions: This symptom is observed when all of the following conditions are present:

  - A packet enters with or without an MPLS label.
  - The router tries to send an ICMP packet to the source in any of the following situations:
    * The packet is denied by an output security ACL.
    * There is no route in the router to forward the packet.
    * The time to live (TTL) of the packet expires.
    * The packet is an ICMP echo request packet, and the router tries to send an ICMP echo reply packet to the source.
  - On the interface on which the packet enters, the **ip unreachable** command is enabled by default.

  Workaround: Enter the **no ip unreachable** command on all interfaces of the router, which works in the following two cases:

  - The packet is denied by an output security ACL.
  - There is no route in the router to forward the packet.

  For other cases, there is no workaround.

- CSCin24544

  Symptoms: A permanent virtual connection (PVC) configuration is removed if a PVC fails when it is recreated.

  Conditions: This symptom is observed on a Cisco 7500 series that has a Versatile Interface Processor (VIP). The PVC configuration may be removed if the VIP is carrying data traffic and the parameters of the virtual circuit (VC) class that is attached to the configured PVCs on the associated interface are modified.

  Workaround: There is no workaround.

- CSCin67400

  Symptoms: Traffic and pings fail when FRF.12 is configured on a POS link.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-POS-2OC3 port adapter.

  Workaround: There is no workaround.

- CSCin72219

  Symptoms: If you enter the **shutdown** command followed by the **no shutdown** command on an interface, traffic that congests the interface may cause the router to crash.

  Conditions: This symptom is observed when a policy is attached to the interface.

  Workaround: There is no workaround.

- CSCin73658

  Symptoms: A Cisco 7500 series fails to handle IP packets with a size of 1499 or 1500 bytes if these packets are received over a PPP Multilink interface.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S when distributed multilink is configured.

  Workaround: There is no workaround.

- CSCin73703

  Symptoms: A router may crash when you enter the **set fr-fecn-becn** command.

  Conditions: This symptom is observed when you enter the **set fr-fecn-becn** command for an unsupported interface (that is, a non-Frame Relay interface).

  Workaround: There is no workaround.

- CSCin74920

  Symptoms: A spurious memory access may occur when a VC class with OAM parameters is created.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

- CSCin76900

  Symptoms: A PA-A3-8T1IMA or PA-A3-8E1IMA port adapter that is installed in a Cisco 7xxx series may display an increasing "rx_no_buffer" counter in the output of the **show controllers atm** privileged EXEC command, and some PVCs that are configured on the port adapter may stop receiving traffic.

  Conditions: This symptom is observed when there is a high-traffic load on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter, or as an alternate workaround, reset the VIP or FlexWAN.

- CSCin77221

  Symptoms: You can configure color-aware policing classes by entering the **match-fr-dlci** command but the command does not have any effect. The **match-fr-de** command works fine.

  Conditions: This symptom is observed when you configure color-aware policing on an edge interface of a PE router.

  Workaround: There is no workaround.

- CSCuk51177

  Symptoms: You may not be able to make a Telnet connection to a Cisco IOS platform.

  Conditions: This symptom is observed when the CNS Exec Agent is used to remotely issue an interactive CLI command.

  Workaround: There is no workaround.

- CSCuk51269

  Symptoms: Multicast packets such as HSRP and OSPF are not received on a port-channel interface.

  Conditions: This symptom is observed when a port-channel interface is configured on a Cisco router, when you reload the router, and when the first member is added to the port-channel interface by entering the **no shutdown** interface configuration command on physical interface.

  Workaround: Enter the do **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port-channel interface.

Wide-Area Networking

- CSCdx84284

  Symptoms: A router may not recognize some inbound Multiprotocol Label Switching (MPLS)-tagged packets that are sent via Frame Relay. Because the router cannot recognize the inbound MPLS-tagged packets, MPLS cannot switch those packets to the outgoing interface. The MPLS-tagged packets are dropped by the router, and the router does not increment the input-packet counter in the output of the **show frame pvc** output EXEC command.

  Conditions: This symptom is observed on a Cisco router that has Cisco Express Forwarding (CEF) enabled and that is running Cisco IOS Release 12.2(7b). The symptom may also occur in other releases.

  Workaround: Enable the **debug mpls packets** EXEC command.

- CSCec55849

  Symptoms: Packets may not be resequenced within a Multilink Frame Relay (MFR) bundle. This situation may have a negative impact on some protocols and applications such as VoIP.

  Conditions: This symptom is observed on nondistributed Cisco platforms such as the Cisco 2600 series. The symptom does not affect distributed Cisco platforms such as the Cisco 7500 series and the Cisco 12000 series.

  Workaround: There is no workaround.

- CSCed02028

  Symptoms: A router may reload unexpectedly because of a bus error after the following error message is displayed:

  ```
  %ATMPA-3-BADVCD:ATM[int] bad vcd [number] packet -
  ```

  Conditions: This symptom is observed on a Cisco router that is configured with an ATM interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an ATM interface when a packet that contains a virtual circuit descriptor (VCD) that is out range is passed on to the ATM driver of the interface in order to be transmitted.

  Workaround: There is no workaround.

- CSCed21813

  Symptoms: A Cisco 7204VXR in which an enhanced 1-port ATM OC-3c/STM-1 port adapter (PA-A3-OC3) is installed may reload unexpectedly because of a bus error. However, the cause of the symptom may be a segmentation and reassembly (SAR) chip failure that occurs because of an "Address Error (store) exception".

  Conditions: This symptom is observed on a Cisco 7204VXR that is configured for Dynamic Bandwidth Selection (DBS) support when you attempt to modify the VC QoS parameters under high traffic conditions.

  Workaround: Shut down the ATM interface before attempting to modify the VC QoS parameters.

- CSCee15586

  Symptoms: A Cisco 7500 series may crash when you configure a T1 channel group.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or 12.0(27)S when the same channel group was previously configured for Frame Relay encapsulation, when one or more PVCs on the channel group were configured on the main interface with a map class that contained a service policy, when the channel group was deleted, and when the map class definition that it referenced was also deleted.

Workaround: Remove the Frame Relay encapsulation before you delete the channel group.

- CSCee53018

  Symptoms: When you enter the **show frame-relay lmi** command on a router, the router may crash, or alignment errors may occur.

  Conditions: This symptom is observed after you first have deleted an MFR interface on the router.

  Workaround: There is no workaround.

- CSCee62222

  Symptoms: The **frame-relay interface-dlci** command is removed unexpectedly from a point-to-point subinterface.

  Conditions: This symptom is observed when you enter the **clear frame-relay-inarp** command.

  Workaround: Do not use the **clear frame-relay-inarp** command.

- CSCee85213

  Symptoms: A spurious memory access may occur and the following error message is generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x60C19208 reading 0x1C
  ```

  Under high-traffic conditions, the console freezes because of an alignment error.

  Conditions: These symptoms are observed on a Cisco 7200 series when a FR-FR local switched connection is configured by entering the **connect** command, when a queuing service policy is enabled on the main interface, and when the DLCI on the outgoing interface does not exist on the incoming interface.

  Workaround: Enter the **frame-relay route** command instead of the **connect** command. If the **connect** command is needed for access to features like policing, the errors do stop if the DLCI on the outgoing interface also exists on the incoming interface that has the service policy. The DLCI can be created under a subinterface that is shut down and that has no IP address configured if it is not used to handle traffic.

- CSCin74785

  Symptoms: A VIP crashes with the following error message:

  ```
  VIP-3-SYSTEM_EXCEPTION: VIP System Exception occurred sig=10, code=0x8
  ```

  Conditions: This symptom is observed when you remove a Frame Relay local switching connection from an MFR interface while traffic is running.

  Workaround: Shut down the connection or interface and ensure incoming traffic has stopped before you remove the connection.

Resolved Caveats—Cisco IOS Release 12.0(28)S6

Cisco IOS Release 12.0(28)S6 is a rebuild of Cisco IOS Release 12.0(28)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(28)S6 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdu32036

  Symptoms: When you attempt to apply an access list for SNMP by entering the **snmp-server tftp-server-list** command, the access list is not applied. This situation makes it possible to copy the configuration to and from any server, regardless of the contents of the access list.

  Conditions: This symptom is observed on a Cisco platform that is configured for SNMP.

  The following sample configuration causes the platform to reject configuration file transfers via SNMP from all hosts except the TFTP server that is specified in access list 5:

  ```
  snmp-server tftp-server-list 5
  ```

  ```
  access-list 5 permit 10.1.1.1
  snmp-server community private RW 5
  snmp-server tftp-server-list 5
  ```

  Workaround: Apply a more general access list to restrict traffic to and from the affected platform.

  Alternate Workaround: Disable the SNMP.

- CSCsb08386

  Symptoms: A router crashes when you enter the **show ip bgp regexp** command.

  Conditions: This symptom is observed on a Cisco router when BGP is being updated.

  Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCsb98906

  Symptoms: A memory leak may occur in the “BGP Router” process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

  Workaround: Disable the **bgp regexp deterministic** command.

IP Routing Protocols

- CSCef08797

  Symptoms: A router may stop redistributing static routes into BGP.

  Conditions: This symptom is observed when the static routes are inserted into the BGP table with a network statement that uses a route map that is configured with the **match as-path** route-map configuration command.

  The symptom occurs because the **match as-path** route-map configuration command causes a non-BGP route to be denied.

  Workaround: Do not use BGP-specific match statements when you source non-BGP routes.

- CSCeg49796

  Symptoms: Commands on a router may be unexpectedly removed from the running configuration.

  Conditions: This symptom is observed on a router that is assigned as a neighbor to a BGP peer group. For example, when the **shutdown** command was previously configured on the router, the command is removed from the running configuration after the router is assigned as a neighbor to a BGP peer group.

  Workaround: Re-enter the commands on the router.

- CSCei16615

  Symptoms: A neighbor reloads when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of an LSP router that functions as a tunnel headend.

  Conditions: This symptom is observed when the following events occur:

  – The tunnel headend sends a Path via RSVP to the neighbor but the Resv message is delayed.
  – There is only one Path to the neighbor for the session.
  – At the neighbor, the cleanup timer for the Path expires before the Resv message arrives, causing the session to be terminated.

  Workaround: There is no workaround.

- CSCsb36755

  Symptoms: When BGP receives an update that has a worse metric route than the previously received route for equal-cost multipath, the BGP table is updated correctly but the routing table is not, preventing the old path from being deleted from the routing table.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP multipath.

  Workaround: Enter the **clear ip route** *network* command.

- CSCsb54823

  Symptoms: One router (R2) may begin sending updates to another router (R1) before R2 has received the BGP prefix list from R1.

  R1 does apply its inbound BGP prefix list so routes are denied if they need to be. However, R2 sends routes to R1 which are denied by R1.

  Conditions: This symptom is observed when both routers have negotiated a BGP outbound route filter (ORF) and when R1 sends its BGP prefix list to R2.

  Workaround: There is no workaround.

- CSCsb74708

  Symptoms: An OSPF sham link may not form an adjacency.

  Conditions: This symptom is observed when there is an interface in the global route table that has an IP address that matches the IP address of the OSPF sham link neighbor.

  Workaround: Reconfigure the routers so that the IP address of the OSPF sham link neighbor does not match any IP addresses of interfaces in the global route table.

  Alternate Workaround: Shut down the interface or change the IP address of the interface in the global route table.

- CSCsb79749

  Symptoms: The output of the **show memory summary** command may contain garbled characters in the “What” column.

Conditions: This symptom is observed when you configure OSPF with at least one network, and then unconfigure it.

Workaround: There is no workaround.

ISO CLNS

- CSCei58655

  Symptoms: A route that fails remains in the routing table with its old metric, preventing an alternate route from being used and causing a routing loop.

  Conditions: This symptom is observed in a network that is configured for IS-IS and iSPF when the IP routes that are advertised in an LSP (irrespective of whether or not the LSP is fragmented) do not age-out during a rerouting failure.

  Workaround: Remove iSPF from the IS-IS process by entering the **router isis** command followed by the **no ispf** command.

Miscellaneous

- CSCdz83100

  Symptoms: High CPU use may occur at the interrupt level on an ingress port adapter or line card that is configured for hardware multicast when there is a high multicast traffic rate.

  Conditions: This symptom is observed when policy-based routing (PBR) matches the multicast traffic and when a switchover to another interface occurs.

  Workaround: Change the deny statement in the PBR configuration so traffic for multicast destination addresses is denied earlier.

  Alternate Workaround: For a short while, remove the PBR configuration from the ingress interface to enable multicast traffic hardware forwarding to be established.

  Further Problem Description: PBR should not influence multicast traffic and it does not when traffic is switched in the hardware. When a switchover to a new interface occurs, multicast packets are initially forwarded in the software until hardware forwarding can take over. PBR interferes with the initial software-switched packets and prevents hardware entries from being created.

- CSCeb06452

  Symptoms: When multicast IP version 6 (IPv6) Cisco Express Forwarding (CEF) is enabled, packets (greater than or equal to 232 bytes) that are forwarded may be corrupted.

  Conditions: This symptom is observed on all Cisco platforms during normal multicast CEF software forwarding.

  Workaround: Use process switching.

- CSCed66490

  Symptoms: When all the physical links of a multilink bundle go down, the bundle bandwidth is set to zero. This situation has two known consequences:

  1. The distributed CBWFQ that is applied on a multilink bundle causes a VIP to crash.
  2. OSPF is unable to calculate the interface cost correctly and generates an error message.

  Conditions: These symptoms are observed on a Cisco 7500 series and Cisco 7600 series that are configured for distributed multilink PPP or distributed multilink Frame Relay.

  Workaround: There is no workaround.

- CSCee22454

  Symptoms: If a packet comes in through an interface on which RPF is enabled and the RPF check lookup results in a default prefix which has the Leaf NULL bit set, the packet is dropped even though the Leaf pointers are valid.

  You can see the RPF drops by entering the **show hardware pxf interface** *interface-number* **detail | inc RPF** command.

  Conditions: This symptom is observed when a Cisco 10000 series has two paths in the routing table installed for the default prefix 0.0.0.0/0 and when the default prefix is a recursive route. This will cause the Leaf NULL bit to be set. The Leaf NULL bit is only used by the RPF check, hence if a packet arrives on an RPF-enabled interface and the RPF check lookup results in the default prefix, the packet is dropped since the Leaf NULL bit is set.

  Workaround: Avoid loadsharing, that is, ensure that there is only one path.

- CSCef94525

  Symptoms: A port adapter that is installed in a VIP or FlexWAN and that is configured with more than 38 multilink bundles may crash.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series when distributed CEF switching is disabled either through entering the **no ip cef distributed** command or through a FIB-DISABLE event.

  Workaround: There is no workaround.

- CSCef98037

  Symptoms: Incoming multicast traffic that is forwarded via the main interface of a Cisco 10000 series is dropped.

  Conditions: This symptom is observed on a Cisco 10000 series that has a Gigabit Ethernet main interface that is configured with a number of VRF-enabled VLAN subinterfaces.

  Workaround: Remove the VRFs from the VLAN subinterfaces.

- CSCeg12134

  Symptoms: When you send multicast traffic over an IPSec tunnel, a memory leak may occur on a router.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3T when both IP CEF and hardware encryption are configured. The symptom may also occur in other releases.

  Workaround: Switch to software encryption for a while and then switch back to hardware encryption.

  Alternate Workaround: Disable IP CEF.

- CSCeh13895

  Symptoms: When a 4-port OC-12 ATM ISE line card is deployed in the core between a P router and a PE router that performs decapsulation in a multicast VPN topology, packets with a size that is larger than 4447 bytes and that need fragmentation are not received by a CE router.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S2 or a later 12.0S release.

  Workaround: There is no workaround.

- CSCeh27783

  Symptoms: A router crashes after you have manually configured 237 IPv6 tunnels.

Conditions: This symptom is observed on a Cisco platform that is configured for IPv6 when there are more than eight paths for one IPv6 prefix. The symptom is platform-independent and not release-specific.

Workaround: There is no workaround.

- CSCeh50638

  Symptoms: A 4-port Gigabit Ethernet ISE line card may crash.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast traffic.

  Workaround: There is no workaround.

- CSCei01644

  Symptoms: A 3-port Gigabit Ethernet (3GE-GBIC-SC) line card that is configured for Fast-Path Multicast Forwarding may reset when receiving specific packets. However, it is not necessary that the line card will crash all times. The resulting action on these packets could result in a simple drop as well.

  Conditions: This symptom is observed on a Cisco 12000 series when a packet with an IP destination address from the reserved multicast range (224.0.0.xxx) and a TTL larger than 1 is received on the 3GE-GBIC-SC line card and when multicast hardware acceleration is enabled.

  Normally, the TTL should be 1 if the destination address is part of the reserved multicast range.

  Workaround: Enter the **no hw-module slot** *slot-number* **ip multicast hw-accelerate source-table size 16 offset 0** command.

- CSCei07805

  Symptoms: When a router has a large VRF configuration and a lot of routing information, the following error messages may be generated during an SSO switchover:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot/cpu 5/0: keepalive failure
  ```

  The following CPUHOG error message and traceback may also be generated:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000) msecs
  (272/145),process = IPC LC Message Handler.

  -Traceback= 40EAF5D8 411DBE94 411DBFB8 411DC5D0 411DEFEC 411DEE90 411E0200 41093100
  410932B8
  ```

  After the FIBDISABLE error messages has been generated, the router may no longer function properly.

  Conditions: This symptom is observed on a Cisco 7600 series but is platform-independent.

  Workaround: There is no workaround.

- CSCei19563

  Symptoms: A faulty PRE may unexpectedly switch from standby mode to active mode, causing the active PRE to crash.

  Conditions: This symptom is observed on a Cisco 10000 series that has dual PREs and that runs Cisco IOS Release 12.0(25)SX6 but may also occur in Release 12.0S.

  Workaround: Remove the faulty PRE.

- CSCei30764

  Symptoms: A PE router that is configured with many (100 or more) Multicast VRFs (mVRFs) may create multiple MDT tunnels for one mVRF.

Conditions: This symptom is observed when you reload a Cisco router that functions as a PE router and that is configured for MVPN.

Workaround: There is no workaround.

- CSCei35132

  Symptoms: When a link failure occurs between two provider (P) routers, the LSP that is protected via Fast Reroute (FRR) for a primary tunnel and the directed LDP session within the tunnel are fast-rerouted onto an assigned backup tunnel. However, when the backup tunnel goes down, VPN prefixes that are protected by backup TE LSP entries in the LFIB become "Untagged." This situation causes packet loss for AToM and L3VPN traffic that uses the link between the P routers as its primary path.

  Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S, that functions as a P router, and that is connected to another P router via a 4-port OC-3 ISE line card.

  The topology is as follows:

  ```
  PE ------ P --- OC-3 --- P ------ PE
  ```

  There are one-hop primary tunnels between every pair of routers that is listed above, and each link is protected by an NHOP backup tunnel LSP.

  The symptom occurs when you pull the TX fiber cable from the 4-port OC-3 ISE line card that forms the protected link between the two P routers, when the protected LSP is fast-rerouted onto the backup tunnel, and when the backup tunnel is torn down. One P router may show "Untagged" entries in its LFIB, especially for a loopback interface to a provider edge (PE) router. This situation breaks the forwarding for all of the L2 and L3 VPNs that depend on that PE router.

  The symptom is timing-dependent. The symptom does not occur all the time and does not seem to be Cisco 12000 series line card-dependent, nor is it specific to a link between the two P router because the symptom may also occur when you pull the TX fiber cable of a line card that forms the link between a PE router and a P router.

  Workaround: There is no workaround.

- CSCei38116

  Symptoms: ISE line cards crash when a Cisco 12000 series receives 640,000 multicast streams.

  Conditions: This symptom is observed when the memory of the ISE line cards becomes exhausted when the thousands of multicast streams are received.

  Workaround: There is no workaround.

- CSCei41469

  Symptoms: The standby PRP crashes when you apply an IPv6 ACL on an interface of an ISE line card.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured with redundant PRPs.

  Workaround: There is no workaround.

- CSCei48972

  Symptoms: After a manual switchover occurs in RPR+ mode, a VPN that is configured on a Frame Relay subinterface fails to recover and CEF may be disabled on line cards.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(30)S2.

  Workaround: Enter the **hw-module slot** *slot-number* **reload** command.

- CSCei52380

  Symptoms: The entry for a tunnel is missing from the mplsOutSegmentTopLabel column of the MPLS-LSR-MIB.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 when a mibwalk is performed on the mplsOutSegmentTopLabel object. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCei54336

  Symptoms: An MPLS LER does not impose labels for traffic that follows the default route, causing traffic to be forwarded via IP.

  Conditions: This symptom is observed on a Cisco 12000 series when the default route has two equal paths, when the ingress line card is an ISE line card, and when the default router is learned via OSPF. The symptom may also occur for other protocols.

  Workaround: Use a single path for the default route. If this is not an option, there is no workaround.

- CSCei62762

  Symptoms: Router may generate and/or forward crafted IP packets with the source IP address being the routers tunnel interface for GRE or mGRE tunnels. Incorrect packet decoding may be seen with "debug tunnel."

  Conditions: The router needs to receive a specially crafted GRE packet sent to the tunnel end-point. The outer IP packet must come from the configured tunnel source and be sent to the configured tunnel destination IP address Present Routed bit must be set to 1.

  Workaround: Upgrade Cisco IOS to a version containing fixes for: CSCuk27655 or CSCea22552 or CSCei62762.

  Further information: On the 6th September 2006, Phenoelit Group posted an advisory:

  * Cisco Systems IOS GRE decapsulation fault

  Cisco's statement and further information are available on the Cisco public website at:

  http://www.cisco.com/warp/public/707/cisco-sr-20060906-gre.shtml

- CSCei71659

  Symptoms: SNMP polling returns a "no such instance" response. This is improper behavior: instead of the "no such instance" response, a counter should indicate zero.

  Conditions: This symptom is observed on a Cisco 7500 series when a class is defined in an input policy map but no traffic has been sent to that class. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCei83644

  Symptoms: A nondefault configuration becomes lost for a serial interface on a channelized OC-48 ISE line card or on a 4-port OC-12 ISE line card.

  Conditions: This symptom is observed on a Cisco 12000 series after you have reloaded the router.

  Workaround: There is no workaround.

- CSCei84343

  Symptoms: IP packets that are forwarded from an Engine 6 interface on a Cisco 12000 series to an iBGP route may not reach the destination node.

Conditions: This symptom is observed when the Engine 6 interface forwards these packets as IP packets even though there is a labeled path to the BGP next hop. The output of the **show cef** command shows that the router uses the MPLS labeled path but the Engine 6 hardware is programmed to forward the packets as IP packets instead of MPLS packets. The next router that receives these IP packets may drop them because the next router may be unaware of the iBGP route.

Workaround: There is no workaround.

- CSCei85758

  Symptoms: Traffic is not forwarded when you enter the **hw-module slot** *slot-number* **np mode feature** command on an ISE line card that is configured for MVPN.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 and that functions as a PE router that performs encapsulation.

  Workaround: There is no workaround.

- CSCei90536

  Symptoms: mVPN packets have corrupted encapsulation headers.

  Conditions: This symptom is observed on a Cisco 12000 series that has a channelized ISE ingress line card when packets are replicates to a VRF interface on the ingress line card, to a VRF interface on another line card, and to a core interface on a third line card. This symptom occurs only after some redundancy switchovers.

  Workaround: Reload the line card.

- CSCei90588

  Symptoms: A bad checksum error, bad LLS TV length error, or both are reported on a router that is configured for OSPF and BGP. These protocols or other configured protocols may flap during the errors, and data packets that are sent to the PRP may be lost.

  Conditions: These symptoms are observed on a Cisco 12000 series that is configured with a PRP-1 when the following conditions are present:

  – OSPF, BGP, and other control protocols are configured with scaled routes and peers.
  – Congestion occurs on the PRP-1 because control packets are targeted to the PRP-1 or because other packets are sent to one of the IP addresses of the router and are terminated on the PRP-1. This situation occurs, for example, when IP ping packets are directed towards one of the loopback addresses and are terminated on the PRP-1.

  Workaround: There is no workaround.

- CSCej00097

  Symptoms: Interfaces on a Cisco 10000 series 1-port channelized OC-12 line card may take too much time to recover after an PRE switchover has occurred.

  Conditions: This symptom is observed when the line card is configured with E1 interfaces that function in SDH mode and is most likely to occur when the line card was previously configured with T1 interfaces that functioned in SONET mode. When a PRE switchover occurs, it may take as long as 60 seconds for all of the interfaces to come back up.

  Workaround: There is no workaround.

- CSCej01743

  Symptoms: Traffic drops may occur when traffic is sent over MFR or Frame Relay links.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 or a later release and that is configured for software forwarding.

Workaround: There is no workaround.

- CSCej04738

  Symptoms: After you have reloaded the router, an input service policy on an interface of a 1-port channelized OC-12 ISE line card that is configured for MLP may become stuck in the suspended mode.

  Conditions: This symptom is observed on a Cisco 12416 that runs Cisco IOS Release 12.0(28)S4 and that is configured with two Performance Route Processors (PRP-1s), one 1-port channelized OC-12 ISE line card, one 4-port OC-3 POS ISE line card, two 1-port OC-48 POS ISE line cards, three OC-192 POS E4+ line cards, and one 4-port GE ISE line card.

  Workaround: Delete and reconfigure the service policy.

- CSCej07539

  Symptoms: Multicast traffic does not resume fully after you have removed the active PRP from the router.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S4 and that is configured with redundant PRPs that function in RPR+ mode. The router has two channelized OC-12 line cards that are configured with mVPNs.

  Workaround: There is no workaround.

- CSCej12324

  Symptoms: A Cisco 10000 series drops a packet for a prefix with an incomplete CEF adjacency.

  Conditions: This symptom is observed when the PXF engine does not punt the packet with the incomplete CEF adjacency to the RP (as it is supposed to do) but drops the packet.

  Workaround: Send a ping for the prefix with the incomplete CEF adjacency in order to complete the CEF adjacency.

- CSCej14847

  Symptoms: Auto-RP messages from a CE router are lost.

  Conditions: This symptom is observed when you enter the **clear ip mroute *** on a connected PE router. The messages do not recover by themselves.

  Workaround: To restart Auto-RP messages, enter the **clear ip mds linecard** command.

  Alternate Workaround: To restart Auto-RP messages, debug the VRF Auto-RP by entering the **debug ip pim vrf** *vrf-name* **auto-rp**.

- CSCej15682

  Symptoms: When multicast traffic is being sourced from different sources, and one of the sources is removed, the **show ip mroute vrf** command for the VRFs still shows that source as active.

  Conditions: This symptom is observed when a source is no longer active when using the **show ip mroute vrf** command.

  Workaround: There is no workaround.

- CSCej20986

  Symptoms: An Engine 4 ingress line card may enter an incorrect carving state in which it sends all packets that are larger than 608 bytes to the buffer size pool (freeq) of the wrong egress line card, causing all packets that are larger than 608 bytes to be dropped. The symptom is especially noticeable when the egress line card is an Engine 2 line card.

  Conditions: This symptom is observed rarely on a Cisco 12000 series.

  Workaround: Reload the Engine 4 ingress line card.

- CSCej22910

  Symptoms: Multicast traffic does not reach a CE router that is connected via static IGMP joins to a PE router.

  Conditions: This symptom is observed when the following conditions are present:

  - Traffic from the PE router that performs encapsulation flows towards the CE router.
  - The PE router that performs decapsulation has an egress line card with one interface connected to the core of the network and another interface connected to the edge of the network.
  - The PE router that performs decapsulation has static joins that are configured for Source Specific Multicast (SSM).

  Workaround: There is no workaround.

- CSCej32588

  Symptoms: An interface of an Engine 6 line card is no longer shut down after an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series when the following events occur:

  1. The interface of the Engine 6 line card is configured with the **no shutdown** interface configuration command in the startup configuration.
  2. The router is reloaded and you verify that the interface comes up.
  3. You enter the **shutdown** interface configuration command on the interface.
  4. You enter the **write memory** command.
  5. You enter the **redundancy force** command.

  After the new RP comes up, the interface appears no longer shut down and the interface comes up again.

  Workaround: After you have entered the **shutdown** interface configuration command on the interface followed by the **write memory** command, reload the router.

- CSCej42144

  Symptoms: A service policy on an Engine 4 + or Engine 6 line card is incorrectly rejected with the following error message:

  ```
  %E4P and E6 LC requires to configure POLICE and SET %command in every class if either
  of these two commands %is configured in class-default class
  ```

  This situation occurs when a **set** command is used in all classes.

  Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(28)S3, that is configured with dual Performance Route Processors (PRP-1s) that operate in SSO mode, and that has multiple E4+ and/or Engine 6 line cards.

  Workaround: There is no workaround.

- CSCej62308

  Symptoms: A ROM monitor upgrade may not take effect.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 and that is configured with a single PRP or two PRPs.

  Workaround: There is no workaround.

- CSCej69557

  Symptoms: After you reload a PE router that functions in an MVPN topology and that is configured for sparse mode and Auto-RP, the router may not learn the Auto-RP that is advertised by both a local and remote CE router, preventing traffic from resuming to flow.

  Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(32)S and that functions as a PE router. The symptom may also occur in other releases of Release 12.0S.

  Workaround: Enter the **clear ip mds line** command.

- CSCej82265

  Symptoms: An MPLS TDP peer is down.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S3 and that has the **mpls ldp protocol tdp** command configured on the interface on which TDP peering cannot be established. The peer router has the **mpls ldp protocol both** command configured.

  Workaround: Enter the **mpls ldp protocol tdp** command on the peer router. Note that this workaround may not be plausible for routers that run a legacy Cisco IOS software that only supports TDP.

- CSCej86175

  Symptoms: In a multicast VPN (MVPN) environment, when a Stateful Switchover (SSO) occurs on a PE router, the multicast traffic in the MVRF does not recover because the neighboring PE router fails to re-establish its PIM neighbor relationship. Note that the symptom does not occur for unicast traffic.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S2 or an interim release for Release 12.0(32)S and that functions as a PE router (PE1) in the following topology:

  ```
  multicast origination --> PE2 --> PE1 --> CE1 --> multicast termination
  ```

  When an SSO occurs on PE1, PE2 does not re-establish its PIM neighbor relationship with PE1 in the MVRF. PE1 and PE2 are global PIM neighbors.

  Workaround: Reload PE1.

  Further Problem Description: When the symptom occurs, PE1 still shows PE2 as its PIM neighbor in the MVRF. Clearing the multicast route in the MVRF does not help to resolve this issue.

- CSCin79691

  Symptoms: QoS information disappears from a FlexWAN module or VIP that is configured with a distributed MFR interface.

  Conditions: This symptom is observed after the FlexWAN module or VIP resets or after the interface flaps.

  Workaround: Remove the service policy from the interface and reapply it to the interface.

- CSCin96583

  Symptoms: After an OIR of a VIP on a Cisco 7500 series, MLP traffic causes a very heavy CPU load on the RP, in turn causing failures in the IPC configuration and memory allocation (malloc) failures.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a large number of distributed MLP bundles.

  Workaround: There is no workaround.

- CSCin96590

  Symptoms: A VIP crashes at the “free_wred_stats” function during an RPR+ switchover.

  Conditions: This symptom is observed on a Cisco router that is configured with a VIP that has a configuration with about 12 MLP bundles with two T1 members when QoS is applied while traffic is flowing.

  Workaround: There is no workaround.

- CSCin96692

  Symptoms: On a Cisco 7500 series that is configured for dMLP, the txacc values of member interfaces may be wrongly credited to other member interfaces, causing RSP-3-RESTART messages, and finally causing traffic to stop.

  Conditions: This symptom is observed when the member links flap continuously for some time while traffic is being processed.

  Workaround: There is no workaround.

- CSCsa65096

  Symptoms: A router may crash during the boot process when the startup configuration includes the **hw-module shutdown** command.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa51602. Cisco IOS software releases not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCsb04721

  Symptoms: When the Any Transport over MPLS (AToM) feature is enabled on a router, AToM virtual circuits to a peer may not be re-established after an interface flap or after being reconfigured, because the required targeted Label Distribution Protocol (LDP) session is not re-established.

  Conditions: This symptom is observed when LDP is not configured on any interfaces via the **mpls ip** interface configuration command, which is typically the case when MPLS Traffic Engineering (TE) tunnels are used to transport AToM traffic between endpoints and when the **mpls ip** interface configuration command is not enabled on any TE tunnels.

  The symptom occurs in Cisco IOS software releases that include the fix for caveat CSCec69982 when any form of one of the following commands is configured on the router and appears in the running configuration:

  ```
  mpls ldp explicit-null
  mpls ldp advertise-labels
  mpls ldp session protection
  mpls ldp password fallback
  mpls ldp password option
  mpls ldp password required
  ```

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec69982.

  Workaround: Enter the **mpls ip** command on a TE tunnel interface or temporarily on a physical interface to force LDP to be re-established.

- CSCsb07807

  Symptoms: A Cisco 10000 series unexpectedly drops some traffic after you have entered the **no service-policy** *policy-name* policy class-configuration command.

  Conditions The symptom observed when the policy that is removed is referenced in other policies, such as in policy map “c” in the following configuration example:

```
policy-map p1
   class class-default
      shape 10000
      service-policy c
policy-map p2
   class-default
      shape 20000
      service-policy c
```

  Workaround: There is no workaround.

- CSCsb11124

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  Cisco has published a Security Advisory on this issue; it is available at http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

- CSCsb12969

  Symptoms: All VIPs or FlexWAN modules reload unexpectedly on a platform that is configured for Modular QoS CLI (MQC).

  Conditions: This symptom is observed on a Cisco 7500 series (with VIPs) and a Cisco 7600 series and Cisco Catalyst 6500 series (both with FlexWANs) when the following steps occur while the physical interface is in the UP state:

  1. An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
  2. You remove the policy map from the PVC and attach the same policy map to the main interface.
  3. You remove the policy map from the main interface.

  At this point, all VIPS or FlexWAN modules reload, even though no traffic is being processed during the above-mentioned steps.

  Workaround: There is no workaround.

- CSCsb28139

  Symptoms: An LDP/BGP adjacency is not formed, and a ping does not go through.

  Conditions: This symptom is observed on a Cisco 12000 series that functions in a scaled VPN environment when an Engine 6 line card faces the core of the MPLS network.

  Workaround: Enter the **clear ip route *** command.

- CSCsb46607

  Symptoms: A standby route processor (RP) may crash in the “CEF LC IPC Background” process.

Conditions: This symptom is observed on a Cisco platform when an SSO switchover occurs.

Workaround: There is no workaround.

- CSCsb53420

  Symptoms: Cell loss occurs when bursty VBR ATM traffic is sent through a Cisco 12000 series 4-port ATM OC-12 ISE line card via an L2TPv3 IP tunnel to another 4-port ATM OC-12 ISE line card on another Cisco 12000 series and when the VBR traffic is sent at rates lower than what is configured on the routers (that is, at about 50 percent of the OC-12 line rate).

  Conditions: These symptoms are observed on a Cisco 12000 series that is connected back-to-back via an OC-192 or OC-48 POS link to another Cisco 12000 series.

  Workaround: There is no workaround.

- CSCsb59555

  Symptoms: An Engine 3 or Engine 4+ line card may be stuck in the “request reload” state and CEF may be disabled on the line card, although the CEF table is up, as is shown in the output of the **show cef linecard** command:

```
Slot      MsgSent    XDRSent  Window   LowQ   MedQ  HighQ Flags
 1            8558     719895    4966      0      0      0 up
 2            8560     718293    4966      0      0      0 up
 3            8609     722867    4965      0      0      0 up
 4            8584     721311    4965      0      0      0 up
 5            8597     724307    4965      0      0      0 up
 9            8586     722060    4966      0      0      0 up
 10           8579     720566    4966      0      0      0 up
 11           8566     719086    4966      0      0      0 up
 12           8606     725072    4966      0      0      0 up
 13           8597     723572    4966      0      0      0 up
*7               1          3      24      0      0      0 disabled, rrp hold
 0            4058     359354    4966      0      0      0 up
VRF Default, version 5032, 5024 routes
 Slot   Version    CEF-XDR    I/Fs State    Flags
 1         5032       5016      67 Active   sync, table-up
 2         5032       5016       5 Active   sync, table-up
 3         5032       5016      20 Active   sync, table-up
 4         5032       5016       5 Active   sync, table-up
 5         5032       5016       5 Active   sync, table-up
 9         5032       5016       4 Active   sync, table-up
 10        5032       5016       4 Active   sync, table-up
 11        5032       5016      20 Active   sync, table-up
 12        5032       5016       4 Active   sync, table-up
 13        5032       5016       8 Active   sync, table-up
*7            0          0       4 Active   table-disabled
 0            0          0       5 Active   request reload, table-up
```

  Conditions: This symptom is observed on a Cisco 12000 series after an RPR+ switchover has occurred. However, the symptom is platform-independent and may also occur on another platform that is configured for CEF when an RPR+ switchover has occurred.

  Workaround: Enter the **clear cef linecard** command for the affected line card.

- CSCsb62041

  Symptoms: A newly created channelized interface may show packet and byte counts before any traffic passes through the interface.

  Conditions: This symptom is observed on a Cisco 12000 series. When a channelized interface is deleted, the interface index is released. This interface index may be re-allocated when a new channelized interface is created. The counters that are associated with the index need to be cleared when an interface is deleted so that they are properly initialized if the index is subsequently re-allocated to a new interface.

  Workaround: There is no workaround. Although you can clear the interface counters via the CLI, doing so does not prevent the symptom from occurring because but there is an internal counter that is used in the Tx byte and packet counts and that may cause errors in the calculations.

- CSCsb75433

  Symptoms: Distributed Multilink PPP (dMLP) packets are not switched via dCEF.

  Conditions: This symptom is observed on a Cisco router that is configured with multilink bundles.

  Workaround: There is no workaround.

- CSCsb88214

  Symptoms: SNMP polling via the CBQoSMIB on the cbQosPoliceStatsTable returns no results.

  Conditions: This symptom is observed on a Cisco 7500 series that has policing defined in a class map.

  Workaround: There is no workaround.

- CSCsb98254

  Symptoms: A router may fail when you reload a Gigabit Ethernet (GE) line card or port adapter that has link-bundling enabled.

  Conditions: This symptom is observed on a Cisco router when dot1q is configured on a GE interface of the line card or port adapter and when MPLS is enabled on an uplink.

  Workaround: There is no workaround.

- CSCsc08181

  Symptoms: The PXF engine reloads when you enter the **service-policy output** command.

  Conditions: This symptom is observed on a Cisco 10000 series router when the following conditions are present:

  – The **frame-relay fragment** command is configured on a Frame Relay interface.

  – An output service policy that has the **bandwidth**, **priority**, or **shape** command enabled is applied to a Frame Relay permanent virtual circuit (PVC).

  Workaround: Do not combine interface-based Frame Relay fragmentation with a PVC-based service policy. Rather, either apply both Frame Relay fragmentation and a service policy to the physical interface or apply both Frame Relay fragmentation and a service policy to the Frame Relay PVC.

- CSCsc37404

  Symptoms: An Engine 6 line card may reset with the following error messages:

  ```
  %IPC-5-INVALID: NACK Source Port=0x403F0000
  %MCC192-3-CPU_PIF: Error=0x4
  ```

```
%MCC192-3-CPUIF_ERR: Packet Exceeds Programmed Length.
%GSR-3-INTPROC: Process Traceback= 40D32E5C 406D8CE0
...
```

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2.

Workaround: There is no workaround.

- CSCuk45823

  Symptoms: A reload occurs during high-load IPv6 multicast forwarding. This is due to a corrupted redzone in the packet memory.

  Conditions: This symptom is observed only on the i82543-based Ethernet family of controllers during high-load IP version 6 (IPv6) multicast forwarding.

  Workaround: Disable IPv6 multicast.

Wide-Area Networking

- CSCee44086

  Symptoms: After an RP switchover, a multilink PPP interface cannot forward any traffic.

  Conditions: This symptom is observed on a Cisco 7500 series, Cisco 10000 series, and Cisco 12000 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink PPP interface.

Resolved Caveats—Cisco IOS Release 12.0(28)S5

Cisco IOS Release 12.0(28)S5 is a rebuild of Cisco IOS Release 12.0(28)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(28)S5 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCei40439

  Symptoms: The output of the **show policy-map interface** command for an interface that is configured for Weighted Random Early Detection (WRED) is not correct. The traffic details in the command output should be displayed with respect to the class maps but are not.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(28)S3.

  Workaround: There is no workaround.

- CSCei51304

  Symptoms: A Cisco 10000 series may generate a “c10k_card_send_cmd_common” error message and subsequent tracebacks.

  Conditions: This symptom is observed when the configuration of a 4-port channelized OC-3 line card is removed.

  Workaround: Configure the correct clock source on each SONET controller.

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCei81634

  Symptoms: A Cisco 10000 series may leak packet buffers at a low rate.

  Conditions: This symptom is observed on a Cisco 10000 series that processes multicast packets when WRED is configured on any interface.

  Workaround: Disable WRED.

- CSCsa86214

  Symptoms: Locally-originated and transit packets that are greater than 1599 bytes in length do not leave a router. BGP and other TCP-based protocols that negotiate large MSS values may go down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE or PRE1 and that performs IP fragmentation.

  Workaround: First, enter the **show hardware pxf cpu buffer** or **show pxf cpu buffers** command to verify buffer depletion. Then, perform a microcode-reload of the PXF engine.

- CSCsa95353

  Symptoms: A Cisco 10000 series that is configured with an inbound service policy may generate the following error message:

  ```
  TOASTER-2-FAULT: T0 HW Exception: CPU[t0r1c3] NULLRD at 0x0CD6 LR 0x096E
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S4 and that is configured with a PRE1 when an MPLS-encapsulated IPv4 packet that contains IP options is processed. The symptom may also occur in other releases.

  Workaround: Remove the inbound service policy.

Resolved Caveats—Cisco IOS Release 12.0(28)S4

Cisco IOS Release 12.0(28)S4 is a rebuild of Cisco IOS Release 12.0(28)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(28)S4 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCed44414

  Symptoms: When the slave RSP crashes, a QAERROR is observed in the master console, resulting in a cbus complex. The cbus complex will reload all the VIPs in the router.

  Conditions: This symptom happens when the slave crashes in a period when there is a large number of packets going towards the RSP. A large number of packets go to the RSP when CEF switching is configured or when routing protocol updates are numerous.

  Workaround: There is no workaround.

- CSCee83917

  Symptoms: The RP of a Cisco router may crash when entering the **write memory** legacy command.

  Conditions: This symptom is observed on a Cisco router that has the **snmp mib community-map** command enabled with a very long community string and an engineID. The symptom may also occur when the long community string is removed from the configuration. The symptom does not occur when entering the **copy running-config startup-config** EXEC command.

  Workaround: A community string that is shorter than 40 characters will not cause the symptom to occur.

EXEC and Configuration Parser

- CSCed51952

  Symptoms: A Cisco router may crash when you perform and online insertion removal (OIR) of a line card.

  Conditions: This symptom is observed when an interface on the line card is being configured through the CLI while the OIR of the line card removes the interface.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCef01220

  Symptoms: A Versatile Interface Processors (VIP) with a PA-MC-8TE1 port adapter may report its memory size as unknown even though the VIP appears to function normally, and Distributed Multicast Fast Switching (DMFS) may fail to function properly.

  Conditions: This symptom is observed on a Cisco 7500 series when any of the following conditions are present:

  – The mode of the controller of the PA-MC-8TE1 port adapter is not set to T1 or E1 and you insert or remove another VIP with any port adapter via an OIR.

  – Irrespective of whether or not the mode of the controller of the PA-MC-8TE1 port adapter is set to T1 or E1, you insert or remove a standby RSP via an OIR.

  Workaround: Enter the **card type** {**t1** | **e1**} *slot* [*bay*] command on the PA-MC-8TE1+ port adapter and ensure that none of the controllers on this port adapter are shut down.

- CSCeg03185

  Symptoms: A few permanent virtual circuits (PVCs) go into a stuck state causing OutPktDrops on a Cisco 7200 router.

  Conditions: This symptom occurs on a Cisco 7200 router running Cisco IOS Release 12.2(26) with a PA-A3-T3 ATM interface. The symptom may also occur in other releases.

  Workaround: Remove and re-apply the PVC statement.

- CSCin86455

  Symptoms: Auto-provisioning may be disabled on a Cisco 7200 series that is configured with a PA-A3 port adapter.

  Conditions: This symptom is observed when a VC class that is configured for create on-demand is attached to the main ATM interface and then the create on-demand configuration is removed and re-applied to the VC class.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface of the PA-A3 port adapter.

- CSCsa87986

  Symptoms: A router may intermittently transmit corrupt PPP packets. When you enter the **debug ppp nego** and **debug ppp errors** commands, it appears that "protocol reject" packets are received from the remote end.

  Conditions: This symptom is observed on a Cisco 7500 series that has only one OC3 POS port adaptor per VIP and that is configured for PPP encapsulation.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdz42920

  Symptoms: A router may crash because of a bus error when you configure IP accounting.

  Conditions: This symptom is observed when you enter the **clear ip accounting** EXEC command.

  Workaround: Do not enter the **clear ip accounting** or **show ip accounting** EXEC command.

- CSCea31201

  Symptoms: A Cisco router may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that has the **ip accounting** interface configuration command enabled.

  Workaround: There is no workaround. The problem is rare and typically not reproducible.

- CSCeg54375

  Symptoms: Routing inconsistencies may occur in the RIB: routes may be missing from the RIB but may be present in the BGP table.

  Conditions: This symptom is observed on a Cisco RPM-XF when the toaster processor crashes. However, the symptom may occur on any platform that has a toaster processor.

  Workaround: Enter the **clear ip route vrf** *vrf-name* ***** command.

- CSCeg89700

  Symptoms: A Cisco router does not recognize an end-of-RIB message from a third-party vendor router and continues to show the "Neighbor is currently in NSF mode" message although the restart procedure of the third-party vendor router is complete.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 BGP peering and NSF. Note that the symptom does not occur when IPv4 BGP peering is configured.

  Workaround: There is no workaround.

- CSCeh16989

  Symptoms: The Multiprotocol BGP (MP-BGP) network entries counter increases above the real number of reachable networks.

  Conditions: This symptom is observed when network activity occurs in a non-converged environment. The correct number of network entries is restored when there is a period of BGP stability that last for about 1 minute or more because BGP is able to converge and the scanner has time to run and collect the old network entries. However, if there is a sustained period of churn and

BGP is only able to converge for a few seconds before new updates arrive, old BGP network entries are not cleaned up, causing the MP-BGP network entries counter to increase above the real number of reachable networks.

Workaround: There is no workaround.

- CSCeh35659

  Symptoms: When the **ip bgp fast-external-fallover permit** interface configuration command is enabled on the main interface of a 4-port Gigabit Ethernet ISE line card and on a subinterface of a connected BGP neighbor, and when you enter the **shutdown** interface configuration command on the main interface, the BGP session that is established on the subinterface remains up for about 150 to 180 seconds before the BGP hold timer causes the session to go down.

  Conditions: This symptom is observed on a Cisco 12000 series only in an per-interface fast external fallover configuration on a 4-port Gigabit Ethernet ISE line card.

  Workaround: There is no workaround. Note that the **ip bgp fast-external-fallover permit** command is currently not supported on subinterfaces.

- CSCeh53906

  Symptoms: A stale non-bestpath multipath remains in the RIB after the path information changes, and BGP does not consider the stale path part of the multipath.

  Conditions: This symptom is observed on a Cisco router that has the **soft-reconfiguration inbound** command enabled and occurs only when the BGP Multipath Loadsharing feature is enabled for three or more paths, that is, the *number-of-paths* argument of the **maximum-paths** *number-of-paths* command has a value of three or more.

  Workaround: Disable the **soft-reconfiguration inbound** command for the neighbor sessions for which the BGP Multipath Loadsharing feature is enabled or reduce the maximum number of paths for the BGP Multipath Loadsharing feature to two.

- CSCei06089

  Symptoms: Conditional advertisement of the default route via a route map does not work when you enter the **neighbor default-originate** command.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP.

  Workaround: Disable the route map entirely. If this is not an option, there is no workaround.

ISO CLNS

- CSCsb07279

  Symptoms: When an IPv4 prefix list is used in a redistribution command for the IS-IS router process, a change in the prefix list is not immediately reflected in the routing tables of a router and its neighbor. The change may take up to 15 minutes to take effect.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S.

  Workaround: To have a change take effect immediately, enter the **no redistribute route-map** command followed by the **redistribute route-map** command for the IS-IS router process.

Miscellaneous

- CSCdw76832

  Symptoms: Some features may not be applied automatically to MLP or MFR interfaces. Also, in complex scaled configurations, CPU hogs may occur on a line card during activation or provisioning of the interfaces.

  Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S and this is configured with a with a 1-port channelized OC-12 (DS1) ISE line card.

  Workaround: There is no workaround.

- CSCec25942

  Symptoms: A POS Engine 2 line card originates a high traffic volume to a downstream router over a POS link because the same packet is sent over and over.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(22)S5.

  Workaround: There is no workaround.

- CSCed13322

  Symptoms: In the **show process memory** command output, the display of total and free memory may show more memory than is actually present in the main processor memory of the router. This is due to an undocumented change in the command output that also includes both processors and I/O memory pools in the amounts allocated by each process and the totals at the top of the output.

  Conditions: This symptom is observed on all Cisco IOS platforms.

  Workaround: Use the output of the **show memory summary** command to determine the individual amounts of total and free memory in each of the processor memory pools and the I/O memory pool.

- CSCee04893

  Symptoms: A Cisco router is not able to forward traffic to a TE tunnel.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(26)S1 or a later release and that is configured for MLP and MPLS, and that has a TE tunnel.

  Workaround: There is no workaround.

- CSCee55068

  Symptoms: On a Cisco router that has L2 PVCs in the AIS alarm state, in addition to sending AIS cells, the router also sends loopback cells to the customer edge router.

  Condition This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S when the **oam-pvc manage** command is configured and when the L2 PVC gets enters the AIS alarm state. However, this caveat is platform-independent.

  Workaround: There is no workaround.

- CSCee55297

  Symptoms: When you suspend and resume the event manager scheduler and an applet tries to register, the registration fails with an error from the operating system.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or Release 12.2S. However, the symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee56252

  Symptoms: An Engine 3 or Engine 5 line card may pause indefinitely when an IPv6 ACL that is configured for security and classification on the line card is modified while being used.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S when the ACL is configured on two or more interfaces of the line card and when IPv6 QoS is configured on these interfaces.

  Workaround: Remove the ACL from the interfaces of the line card before you modify the ACL.

- CSCee93598

  Symptoms: An LSP ping reports that an LSP is fine although the LSP is unable to carry MPLS payloads such as VPN traffic.

  Conditions: This symptom is observed on a Cisco router when MPLS echo request packets are forwarded from untagged interfaces that are directly connected to the destination of the LSP ping and when the IP time-to-live (TTL) value for the MPLS echo request packets is set to 1.

  Workaround: There is no workaround.

- CSCef41934

  Symptoms: A router processes incoming LSP ping packets as unlabeled IP packets on a VRF interface or a non-MPLS interface.

  Conditions: This symptom is observed on a Cisco router that has the MPLS LSP Ping feature enabled.

  Workaround: Use an ACL to block port 3503 that is used for LSP ping packets. However, note that this may prevent some MPLS LSP Ping applications from functioning properly, as noted below:

  LSP ping packets that enter on a VRF interface are dropped because the router uses the global routing table in its attempt to reply to MPLS echo requests, which could cause the reply to be forwarded to the wrong destination.

  LSP ping packets that enter on an interface that is not configured for MPLS are processed, but depending on the type of MPLS echo packet, the following occurs:

  - MPLS echo request packets are dropped.
  - MPLS echo reply packets are not dropped. (It possible for an MPLS echo reply packets to be received on a non-MPLS interface because the reply path is asymmetric with the forward LSP.)

- CSCef52974

  Symptoms: An Engine 3 ingress line card crashes continuously with alpha errors and IPC errors when it processes ingress multicast traffic.

  Conditions: This symptom is observed on a Cisco 12000 series when you reload an Engine 3 ingress line card that has 5000 (S,G) entries.

  Workaround: There is no workaround.

- CSCef56201

  Symptoms: Multicast MAC rewrites are not updated, preventing multicast traffic from being switched.

  Conditions: This symptom is observed when the VLAN encapsulation is changed, for example from dot1q to dot1q, from dot1q to QinQ, or from QinQ to dot1q.

  Workaround: Enter the **clear ip mroute** command.

- CSCef64439

  Symptoms: A PRE requires a long time to enter the STANDBY HOT state after a switchover.

Conditions: This symptom is observed on a Cisco 10000 series when two PREs are forced to switchover back and forth.

Workaround: Enter the **snmp-server ifindex persist** command.

- CSCef70328

  Symptoms: A VPN traceroute is broken, and packets are dropped from a router on which a port channel is configured as the default route.

  Conditions: This symptom is observed on a Cisco router that functions as a CE router on which a port channel is configured as the default route. The adjacency that causes the packets to be dropped is a drop or punt adjacency.

  Workaround: Do not configure a port channel as a default route.

- CSCef87449

  Symptoms: When you enter the **shutdown** interface configuration command on the outgoing interface of a Traffic Engineering (TE) Label Switched Path (LSP), the Resv state should be removed immediately. However, the Resv state remains until a PathTear arrives or a timeout causes the TE LSP to be torn down.

  When the TE headend is a Cisco router, the PathTear is sent very quickly and the state is removed.

  This symptom is short-lived and it is very unlikely to be noticed.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCec26563 when the router has MPLS TE tunnels enabled.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec26563. Cisco IOS software releases not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCef97190

  Symptoms: The "giants" counter increments continuously for a serial T1 interface when MR-APS is configured on a 4-port channelized STM-1 line card. The symptom occurs even when the fiber is pulled from the OC-3 port.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.3(7)XI1 when the serial T1 interface is in the inactive state, irrespective of whether it is the working interface or the protect interface. The symptom does not occur when the serial T1 interface is in the active state, again irrespective of whether it is the working interface or the protect interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg26528

  Symptoms: The performance of a router may be severely degraded (at approximately 90 percent of the line rate) when large packets are processed, when the MLP bundle link flaps, and when the router does not recover the MLP sequence numbers of the packets.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series that are configured for dMLP only when large packets are processed.

  Workaround: There is no workaround.

- CSCeg35670

  Symptoms: Shortly after a Cisco IOS software boot loader image has been downloaded, a PRP-2 may crash and does not reload.

Conditions: This symptom is observed on a Cisco 12000 series that runs the boot loader image of Cisco IOS Release 12.0(30)S.

Workaround: There is no workaround.

- CSCeg82322

  Symptoms: Platform independent multicast protocol software running in a line card will exit without logging any errors when detecting an illegal value for an input “hardware” interface if_index or an input “software” interface if_number.

  A line card may crash or experience other errors whose cause will be difficult to identify.

  Conditions: These symptoms only occur when a preceding error has occurred during route processor assignment of interface indices. These errors are frequently accompanied by error messages.

  Workaround: Utilize RP error messages if available to diagnose the cause of the problem.

- CSCeh04295

  Symptoms: When ATM packets are sent over an 8-port OC-3 ATM Engine 2 line card, the packets are punted to the CPU of the line card, causing traffic drops.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S and that is configured for AToM when an 8-port OC-3 ATM Engine 2 line card is the disposition card.

  Workaround: There is no workaround.

- CSCeh13340

  Symptoms: On a Cisco XR 12000 series hardware-based forwarding line card, the receive counters in the output of the **show mpls l2transport vc** command do not work in any images for AToM.

  Conditions: This symptom is observed on all hardware-based engine line cards on a Cisco XR 12000 series that is configured for AToM and Sampled NetFlow on the core-facing line cards.

  Workaround: There is no workaround.

- CSCeh13919

  Symptoms: A Cisco 12000 series line card may generate the following error message and traceback when you delete MLP bundles:

  ```
  %LC_DMLP-4-BUNDLENULL: Unexpected null bundle in bflc_cx3_dmlp_frag_on_off, searching
  for group13
  -Traceback= 402FFF44 40300228 40E1880C 40E18BE0 40E19900
  ```

  Conditions: This symptom is observed on a Cisco 12000 series when you delete MLP bundles by entering the **copy tftp run** command to copy the configuration script that is supposed to delete the MLP bundles.

  Workaround: There is no workaround. However, the message does not impact any functionality of the router and the router recovers by itself.

- CSCeh14012

  Symptoms: A 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card on a CE router may crash when many (168) MLP interfaces are deleted and reconfigured via TFTP on a directly-connected PE router.

  Conditions: This symptom is observed on a Cisco 1200 series that functions as a CE router.

  Workaround: There is no workaround.

- CSCeh20156

  Symptoms: When the working link flaps with two to three second intervals on CHOC12 Internet Services Engine (ISE) line cards that are configured for automatic protection switching (APS), some T1 links may remain down.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: Reload he line card(s).

- CSCeh23047

  Symptoms: After a manual SSO switchover, traffic in the tag switching-to-IP switching direction between an egress 1-port 10-Gigabit Ethernet Engine 4+ line card and an ingress 4-port Gigabit Ethernet ISE line card does not recover.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S. However, the symptom is platform-independent and may also occur on other platforms that function in a similar configuration and that run other releases.

  Workaround: Reload microcode onto the 4-port Gigabit Ethernet ISE line card.

- CSCeh25739

  Symptoms: High jitter occurs on a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card when when many (168) MLP interfaces are congested with real-time and normal data traffic.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: There is no workaround.

- CSCeh35422

  Symptoms: A PRP switchover causes "%SYS-2-NOTQ" and "%SYS-2-LINKED" error messages and some tracebacks to be generated on a 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card, the serial interfaces of the line card flap, and eventually the line card resets.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or Release 12.0(30)S, that is configured with two PRPs, and that has the redundancy mode set to SSO.

  Workaround: There is no workaround.

- CSCeh39904

  Symptoms: After removing a large number of Frame Relay subinterfaces, the following log is displayed:

  ```
  SYS-3-CPUHOG: Task ran for 38160 msec (3/2), process = MDFS LC Process, PC = 41129150
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for Multicast VPN.

  Workaround: There is no workaround.

- CSCeh46072

  Symptoms: When the following sequence if performed on a Cisco router, multiple subinterfaces receive the same ifIndex number, causing incorrect CEF entries:

  1. Create a serial subinterface (channelized).
  2. Delete the same subinterface.
  3. Create an ATM subinterface.
  4. Re-create the serial subinterface.

  Conditions: This symptom is observed on a Cisco 12000 series when the above-mentioned or a similar sequence of adding and deleting subinterfaces is performed.

Workaround: Do not delete and re-add the same subinterface. Rather, enter the **shutdown** command followed by the **no shutdown** command to achieve the same effect.

- CSCeh60368

  Symptoms: On a Cisco 10000 series that is configured with 6-port channelized T3 line cards, when the primary and standby PREs are each loaded with a different Cisco IOS software release (for example, Release 12.0(28)S and Release 12.0(28)S3) and when the standby PRE boots, the standby PRE may crash or other errors may occur while the standby PRE configures the channelized T3 channels.

  Conditions: This symptom is observed on a Cisco 10000 series for Cisco IOS Release 12.0(27)S, Release 12.0(28)S, Release 12.0(30)S, Release 12.0(31)S or a rebuild of these releases when the standby PRE runs a Cisco IOS software release that is either older or newer than the software release on the primary PRE and when one PRE runs a software release that includes the fix for caveat CSCsa41907 and the other PRE runs a software release that does not contain the fix for caveat CSCsa41907.

  Workaround: Do not perform live software upgrades. Rather, bring the primary PRE down and boot the standby PRE with the same Cisco IOS software release that runs on the primary PRE, so that when both PREs come up, their software releases match.

  Further Problem Description: When both the primary and standby PRE run a Cisco IOS software release that contains the fix for caveat CSCsa41907, the symptom does not occur.

- CSCeh64632

  Symptoms: After a route processor or line card has reloaded, the queue limit that is set for the class default is not properly programmed.

  Conditions: This symptom is observed on a Cisco 12000 series 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that has an egress policy applied to a serial interface.

  Workaround: There is no workaround.

- CSCeh65748

  Symptoms: A Engine 3 ISE line card may not properly handle incoming bad IP packets but may generate a traceback and a transient error message:

  ```
  %GSR-3-INTPROC: Process Traceback= 400E10B4 400FBA2C
  -Traceback= 4047917C 405E5274 400F4B58
  %EE48-3-BM_ERRS: FrFab BM SOP error 40000
  %EE48-3-BM_ERR_DECODE: FrFab SOP macsopi_bhdr_pkt_len_zero_err
  ```

  ```
  %GSR-3-INTPROC: Process Traceback= 400E1090 400FBA2C
  -Traceback= 4047917C 405E5274 400F4B58
  %LC-4-ERRRECOVER: Corrected a transient error on line card.
  ```

  The line card may also crash.

  Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S1 or Release 12.0(26)S5a.

  Workaround: There is no workaround.

- CSCeh76523

  Symptoms: On a Cisco 12000 series with an unidirectional MR-APS configuration, traffic los occurs when the line card that contains the APS protect interface is reloaded.

  Conditions: This symptom is observed mostly in highly-scaled APS configurations on a channelized OC-48 ISE line card that is configured for unidirectional APS.

  Workaround: There is no workaround.

- CSCeh78918

  Symptoms: When a line card has reloaded because you reloaded the router, the line card crashed, or you entered a command to reload the line card, the following message may appear on the console:

  ```
  %MDS-2-RP: MDFS is disabled on some line card(s). Use "show ip mds stats linecard" to
  view status and "clear ip mds linecard" to reset.
  ```

  This message may be generated because MDFS is erroneously disabled on the reloaded line card. Erroneous disabling of MDFS may unnecessarily extend network convergence time.

  Conditions: This symptom is observed on a distributed router or switch such as a (Cisco Catalyst 6000 series, Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series. The symptom occurs when the router has the **ip multicast-routing distributed** command enabled for any VRF and when a line card is reloaded more than 50 seconds into the 60-second MDFS flow-control period.

  Workaround: The symptom corrects itself after 60 seconds. Alternatively, you can enter the **clear ip mds linecard** *slot number* command.

- CSCeh84233

  Symptoms: After a manual switchover on a Cisco 12000 series that has two RPs that runs in RPR+ mode, some MLP bundles on a 1-port channelized OC-12 (DS1/E1) ISE line card may not forward traffic.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S3.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the MLP interface.

- CSCeh84740

  Symptoms: An RPR+ switchover may cause a VIP or line card to pause indefinitely.

  Conditions: This symptom is observed when a high load of traffic passes through interfaces of a VIP or line card when these interfaces are configured for QoS.

  Workaround: There is no workaround.

- CSCeh96621

  Symptoms: The line protocol of interfaces goes down, the router is unable to allocate further resources, and the router generates the following error messages:

  ```
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial5/0.8/23:0, changed state to
  down
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial5/0.8/24:0, changed state to
  down
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Multilink11 0, changed state to down
  %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial5/0.8/25:0, changed state to
  down
  %EERP-2-UIDB_ERR: Unable to allocate resources. Invalid index for free 935
  %EERP-2-UIDB_ERR: Unable to allocate resources. Invalid index for free 926
  %EERP-2-UIDB_ERR: Unable to allocate resources. Invalid index for free 937 ...
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S3 when you use a script that adds and deletes a multilink configuration.

  Workaround: There is no workaround.

- CSCeh97080

  Symptoms: When Multiprotocol Label Switching (MPLS) is enabled on a router, one or more LDP sessions may be disrupted during periods of extremely high CPU use.

Conditions: This symptom is observed when the CPU use of the router temporarily increases to more than 90 percent for several tens of seconds and when one or more high-priority processes are frequently active but do not necessarily use many CPU cycles.

For example, high CPU use may occur when a peer router is reloaded or when an interface with several hundreds of numbered IP subinterfaces comes up, which causes many processing changes on the router because of the "Tagcon Addr" process.

On a Cisco 12000 series, high CPU use may occur because of the "Fabric ping" high-priority process, which is frequently active.

Other high-priority processes may also cause the symptom to occur.

Workaround: To increase the length of the hello adjacency holdtimes, enter the **mpls ldp discovery hello holdtime** command on the affected router. You may need to enter this command on all platforms in the network in order to provide full protection.

- CSCeh97760

  Symptoms: In the outputs of the **show ip psa-cef** and **show ip cef** commands for an Engine 2 ingress line card, the "Local OutputQ (Unicast)" information may point to another and incorrect slot than the slot that the global CEF table points to.

  When this symptom occurs, packets that are destined for these specific IP address are dropped.

  Conditions: This symptom is observed on a Cisco 12000 series when an Engine 2 line card is used as an ingress line card for traffic that is directed to a default route.

  Workaround: Enter the **clear ip route 0.0.0.0** or **clear ip route *** command.

- CSCeh97829

  Symptoms: An RP may crash continuously when you reload all the line cards in a dual-RP router that has the redundancy mode is set to SSO.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured with two GRPs or two PRPs that are configured for SSO and occurs only when a 1-port channelized OC-48 ISE line card, a 4-port channelized OC-12 ISE line card, or 16-port channelized OC-3 ISE line card is present in the router.

  Workaround: Set the redundancy mode to RPR or RPR+.

- CSCei00027

  Symptoms: On a channelized OC-48 ISE line card with APS configured, a "Signal Failure" condition remains after the line card has been reloaded or after you enter the **shutdown** command followed by the **no shutdown** command.

  Conditions: This symptom is observed on a Cisco 12000 series and affects only a channelized OC-48 ISE line card with an APS configuration.

  Workaround: There is no workaround.

- CSCei04350

  Symptoms: MVPN PIM neighbors that are associated with both a 1-port channelized OC-48 ISE line card and a 1-port channelized OC-12 (DS1) ISE line card bounce when you perform a microcode-reload of a 1-port channelized OC-12 (DS1) ISE line card.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: There is no workaround.

- CSCei07556

  Symptoms: The PPP protocols flap on a 64K-port of an interface of a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card that is configured for CoS and that is congested.

  Conditions: This symptom is observed when two Cisco 12000 series are connected back-to-back, when the routers are connected via 1-port channelized OC-12/STM-4 (DS1/E1) ISE line cards, and when you send real-time traffic.

  Workaround: Change the QoS output policy to prevent traffic from being for longer than 10 seconds and enable keepalive packets to time out.

  Further Problem Description: The symptom does not occur when you do not send real-time traffic.

- CSCei07946

  Symptoms: When the active rate for a destination PE router is evenly distributed at 4 pps for 20 flows and the active rate for a destination CE router is evenly distributed at 4 pps for 19 flows, one flow is reported at twice that rate (that is, 8 pps).

  Conditions: This symptom is observed on a Cisco 12000 series that functions in a MVPN VRF-Lite environment with 20 multicast streams that have a single sustained cell rate (SCR) and that have the pps rate evenly distributed across all streams.

  Workaround: There is no workaround.

- CSCei12771

  Symptoms: All traffic with a 0 label plus another label is dropped by a 3-port Gigabit Ethernet egress ISE line card.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S.

  Workaround: There is no workaround.

- CSCei15701

  Symptoms: The active PRP pauses indefinitely after it changes from standby to active.

  Conditions: This symptom is observed when the redundant PRPs are configured for RPR+ mode, the router has two APS-protected CHOC12 line cards, the router has mVPNs configured, and the router runs Cisco IOS Release 12.0(28)S3.

  Workaround: There is no workaround.

- CSCei22697

  Symptoms: Some MVPN tunnels are mapped to an incorrect VRF forwarding table.

  Conditions: This symptom is observed on a Cisco router that is configured for data MDT groups.

  Workaround: There is no workaround.

- CSCei27448

  Symptoms: A router may crash while displaying the output of the **show ip pim mdt bgp** command.

  Conditions: This symptom is observed when withdraws for a MDT source group are received by PIM from BGP while you enter the **show ip pim mdt bgp** command.

  Workaround: There is no workaround. To reduce the chance of the router crashing, change the *screen-length* argument in the **terminal length** *screen-length* command to 0. Doing so prevents the router from pausing between multiple output screens. (The default of the *screen-length* argument is 24.)

- CSCei31560

  Symptoms: On a 6-port channelized T3 line card that has a multilink bundle configured, the delay that occurs for traffic in a priority queue is about 12 to 14 milliseconds more than what you would expect.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S that is configured with a multilink protocol such as MFR or MLP. These protocols and congestion may cause excess delay for priority traffic.

  Workaround: There is no workaround.

- CSCei33908

  Symptoms: mVPN packets have corrupted encapsulation headers.

  Conditions: This symptom is observed on a Cisco 12000 series that has a channelized ISE ingress line card when packets are replicates to a VRF interface on the ingress line card, to a VRF interface on another line card, and to a core interface on a third line card. This symptom occurs only after some redundancy switchovers.

  Workaround: Reload the line card.

- CSCei39383

  Symptoms: Interface configuration parameters are not applied to the running configuration after an RPR+ switchover.

  Conditions: This symptom is observed intermittently on a Cisco 12000 series that is configured with a 1-port CHOC-48 ISE line card but may also occur with other line cards.

  Workaround: Apply the configuration manually to the affected interface.

- CSCei40506

  Symptoms: Performance drops to 90 percent when the “N flag” is set incorrectly for the MDFS process.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for mVPN, that uses an Engine 3 line card for imposition, and that uses an Engine 4+ line card for disposition.

  Workaround: Reload the router.

- CSCei47377

  Symptoms: On a 1-port channelized OC-12 ISE line card, the configuration of an interface that is configured for MFR, MLP, and QoS may become lost during the switchover of an RP.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S and that is configured with two RPs that have the redundancy mode set to RPR+.

  Workaround: There is no workaround.

- CSCsa49906

  Symptoms: When an attempt is made to remove a loopback from a T1 interface of a channelized T3 controller, the following warning message is generated and the loopback is not removed:

  ```
  %Inband loopback is already running on T1 12. Only one code can be running per T3 at
  a time
  ```

  Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S2 and that is configured with a 6-port channelized T3 line card.

  Workaround: There is no workaround.

- CSCei50162

  Symptoms: The physical layer interface module (PLIM) of a 6-port channelized T3 that is configured for MLP may not be updated with MLP link information.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 after you have reloaded the router.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MLP interfaces.

- CSCei51504

  Symptoms: When you run an SNMP get or walk on the ifOperStatus object on a 1-port CHOC-12 OC-3 ISE line card, the status for the STS-1 path interface shows down although the channel is up.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S3.

  Workaround: There is no workaround.

- CSCei66187

  Symptoms: Multilink PPP interfaces flap more than once.

  Conditions: This symptom is observed following an RPR+ switchover for a 1-port ISE OC-12 channelized to DS1/E1 line card that is configured with 168 multilink VRF interfaces, all of which are configured for QoS.

  Workaround: There is no workaround.

- CSCin72437

  Symptoms: A port adapter in a router or FlexWan module in a switch may crash when an SSO switchover occurs on a Route Processor or Supervisor Engine.

  Conditions: This symptom is observed when the port adapter or FlexWan module is configured with a QoS policy.

  Workaround: There is no workaround.

- CSCin91381

  Symptoms: A VIP that has a dMLFR configuration may crash when you enter the **microcode reload** global configuration command.

  Conditions: This symptom is observed on a Cisco 7500 series when traffic flows through the VIP.

  Workaround: There is no workaround.

- CSCsa59109

  Symptoms: At random, subinterfaces loose the ability to ping a directly-connected peer.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured with two 3-port Gigabit Ethernet line cards.

  Note that although regular and extended pings do not work, pings that use the record option do work.

  Workaround: Reload microcode onto the affected line cards.

- CSCsa59829

  Symptoms: With traffic passing over a network only occasionally, a 4-port OC12 ATM ISE line card generates a "%PM622-3-CPK24_INTR: Egr SAR timeout" error message and resets.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: Reload the line card.

Further Problem Description: The symptom occurs when the "CPK24 FPGA" detects that the SAR does not respond in the "Utopia interface." The SAR then crashes because of a bad canonical header in the egress direction.

- CSCsa64476

  Symptoms: A Cisco 10000 series generates the following error message:

  ```
  %GENERAL-3-EREVENT: ACLs could not add IDB to list
  ```

  The message is followed by a traceback.

  This may indicate that the standby PRE does not apply the ACL for security purposes.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs. The symptom is a timing issue.

  Workaround: There is no workaround.

- CSCsa65732

  Symptoms: When you remove a policy map from a subinterface, the subinterface may become stuck, preventing traffic from passing through the subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX7 when a nested policy map is applied to the main or physical interface in addition to the one that is already applied to the subinterface. The symptom could also occur in Release 12.0S.

  Workaround: Remove the policy map from the physical interface before you remove the policy map from the subinterface. When the subinterface configuration is updated, re-apply the policy map to the physical interface.

- CSCsa74044

  Symptoms: An RP crashes during large interface configuration changes when interfaces and QoS policies are added or deleted.

  Conditions: This symptom is observed on a Cisco 12000 series when the configuration changes involve ATM and serial interfaces.

  Workaround: There is no workaround.

- CSCsa77105

  Symptoms: An LSP ping (or traceroute packet) is incorrectly sent from an unlabeled interface, preventing the LSP ping to detect LSP breakages when a one-hop label switched path is pinged.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS OAM.

  Workaround: There is no workaround.

- CSCsa80661

  Symptoms: The data path on a 3-port Gigabit Ethernet Engine 2 (3GE-GBIC-SC) line card may be reset because of a corrupted packet that is found in the Tx SOP SRAM. This situation causes packet loss and the routing protocol sessions to flap.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS software release that includes the fix for caveat CSCef06121. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef06121. Cisco IOS software releases that are listed in the "First Fixed-in Version" field at this location are affected.

  Workaround: There is no workaround. The symptom causes a disruption of service, but service is restored.

Further Problem Description: When the symptom occurs, the following messages are generated in the log:

```
%RP-3-FABRIC_UNI: Unicast send timed out (1)
CORRUPT PACKET DUMP:
000005C000000000 0200000000000000 0000000101000000 00062AD9B40A0003 A09D008208004500
0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000
0000000000000000 0000000000000000

%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/0: Link OK - autonegotiation
complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/2: Link OK - autonegotiation
complete
%RPGE-6-AUTONEG_STATE: Interface GigabitEthernet1/1: Link OK - autonegotiation
complete
%LCGE-3-SOP_BAD_PACKET: Found corrupt pkts in tx-sop-sram. Data path was reset.

%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.38 on GigabitEthernet1/0 from LOADING to
FULL, Loading Done
%OSPF-5-ADJCHG: Process 1, Nbr 10.142.65.44 on GigabitEthernet1/2 from LOADING to
FULL, Loading Done
```

- CSCsa86214

  Symptoms: Locally-originated and transit packets that are greater than 1599 bytes in length do not leave a router. BGP and other TCP-based protocols that negotiate large MSS values may go down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE or PRE1 and that performs IP fragmentation.

  Workaround: First, enter the **show hardware pxf cpu buffer** or **show pxf cpu buffers** command to verify buffer depletion. Then, perform a microcode-reload of the PXF engine.

- CSCsa87295

  Symptoms: Traffic to a network core is dropped from a link-bundle interface of an Engine 3 line card.

  Conditions: This symptom is observed when the network core is a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release, that functions as a PE router, that is configured for MPLS VPN, and that has L3 loadbalancing enabled on an egress path through a link-bundle interface.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs because there is incorrect FCR information in the Engine-3 hardware rewrites that point to the link-bundle interface.

- CSCsa88211

  Symptoms: When you boot a Cisco 12000 series, some Layer 1 and CoS command are rejected with the following error messages:

  ```
  Command "pos threshold sd-ber 9"  not allowed on link-bundle member interface POS1/0
  Command "tx-cos TEST"  not allowed on link-bundle member interface POS1/0
  ```

  Conditions: This symptom is observed on a Cisco 12000 series when a POS interface of an Engine 0 or Engine 2 line card has the **tx-cos** command enabled and is a member of a port channel or POS channel.

  Workaround: There is no workaround.

- CSCsa96941

  Symptoms: When VBR ATM traffic is sent through a Cisco 12000 series 4-port ATM OC-3 ISE line card via an L2TPv3 IP tunnel to another 4-port ATM OC-3 ISE line card on another Cisco 12000 series, the VBR ATM traffic passes at lower rates than what is configured on the routers, and cell loss occurs.

  Conditions: These symptoms are observed on a Cisco 12000 series that is connected back-to-back via an OC-192 POS link to another Cisco 12000 series.

  Workaround: There is no workaround.

- CSCsb00493

  Symptoms: Packets do not switch through a core interface of a line card that has hardware acceleration enabled.

  Conditions: This symptom is observed on a Cisco 12000 series when the line card that contains the core interface has also a VRF interface that is shut down.

  Workaround: Disable hardware acceleration on the line card.

- CSCsb01461

  Symptoms: A 4-port OC-12/STM-4 ATM ISE line card may forcefully reload. The following log message may also be reported after the forceful reload:

  ```
  Linecard Reset with %PM622-3-CPK24_INTR: Egr Mismatch.
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S5.

  Workaround: There is no workaround.

- CSCsb02964

  Symptoms: When a class map that contains an access control list (ACL) that is too large and complex to fit in memory is applied to an MQC policy map on a Cisco 10720, the router pauses indefinitely while compiling the ACL and generates a MALLOCFAIL error. The router should report an out-of-memory situation.

  Conditions: This symptom is observed when the ACL contains 2000 lines and is complex.

  Workaround: There is no workaround.

- CSCsb07591

  Symptoms: On a 1-port OC-48 Engine 3 line card that has 350 Frame Relay subinterfaces on which VRF is enabled, traffic is forwarded on all subinterfaces with the exception of one subinterface.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S and that functions as a CE router when the 1-port OC-48 Engine 3 line card provides a connection to a PE router.

  Workaround: Remove and reconfigure VRF forwarding on the affected subinterface.

- CSCsb08198

  Symptoms: On a Cisco 12000 series that is configured for MR-APS, traffic duplication occurs in the ingress direction on a 1-port channelized OC-12 (DS1/E1) ISE line card.

  Conditions: This symptom is observed after an RP switchover, after the router reloads, or after an APS switchover. The inactive APS interface should drop all ingress traffic, but this does not occur, causing traffic duplication.

  Workaround: There is no workaround.

- CSCsb09190

  Symptoms: A router misses an entry in its label forwarding table, which is shown in the output of the **show tag-switching forwarding-table** EXEC command for the missing entry and in the output of the **show ip cef detail** EXEC command for the prefix.

  Conditions: This symptom is observed on a Cisco router that is configured for Multiprotocol Label Switching (MPLS) and that learns its routes through iBGP from redundant route reflectors (RRs) when BGP labeling is not enabled.

  Workaround: There is no workaround. However, when you enter the **clear ip route** EXEC command for the affected prefix, the prefix is reinstalled in the label forwarding table.

- CSCsb18880

  Symptoms: A 4-port channelized STM-1/OC-3 line card resets and generates an "IRONBUS-FAULT" error message.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **tug-2** *tug-2-number* **e1** *e1-number* **loopback** command on the line card.

  Workaround: There is no workaround.

- CSCsb29326

  Symptoms: An snmpwalk fails for cmplsFrrFacObjects in the FRR-MIB.

  Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S6, Release 12.0(28)S3, or Release 12.0(31)S.

  Workaround: There is no workaround.

- CSCsb33258

  Symptoms: A Cisco 12000 series RP crashes during BGP convergence when MVPNs are configured.

  Conditions: This symptom is observed on a Cisco 12000 series after a duplicate BGP MDT extended community message is received that specifies a different Route Descriptor (RD) for an MDT that already exists for the specified MDT source and group address.

  Workaround: There is no workaround.

- CSCsb41367

  Symptoms: When you enter the **redundancy force-switchover** command, an Engine 4 line card may crash.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz Cisco IOS software image and that has two RPs that function in SSO mode.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCef54653

  Symptoms: Some members of a multilink bundle remain inactive, while others are active.

  Conditions: This symptom is observed when the interfaces are configured with the **ppp chap hostname** or **ppp multilink endpoint** command. Very high speed interfaces may come up and join the multilink bundle faster than the configuration can be processed, which causes them to use the host name of the router (instead of the configured user name or endpoint value) as the Endpoint Discriminator during Link Control Protocol (LCP) negotiations. This situation causes a mismatch between these links and those that come up after the configuration command is processed.

Workaround: Enter the **shutdown** interface configuration command followed by **no shutdown** interface configuration command on the active links to enable the links to renegotiate LCP with the correct Endpoint Discriminator value.

Resolved Caveats—Cisco IOS Release 12.0(28)S3

Cisco IOS Release 12.0(28)S3 is a rebuild of Cisco IOS Release 12.0(28)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(28)S3 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCeg15044

  Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a "No Free TTYs error" message is generated.

  Conditions: This symptom is observed when there are simultaneous Telnet requests.

  Workaround: There is no workaround.

- CSCeg16078

  Symptoms: You cannot create a VRF-aware ICMP, UDP, or jitter probe using SNMP.

  Symptoms: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(27)S. Note that the symptom does not occur in Release 12.2(11)T.

  Workaround: Use CLI commands to create a probe.

- CSCeg41734

  Symptoms: The console of a router may stop responding and the router may stop forwarding traffic.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(6b) and that is configured with an NPE-G1 when the native Gigabit Ethernet interfaces of the NPE-G1 are used.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCin88718

  Symptoms: All channels on a PA-MC-2T3+ port adaptor stop sending traffic although they continue to receive packets. All interfaces will remain in up/down state.

  Conditions: Once we send greater than linerate over the port adaptor, for a little while the PA locks up and never returns to normal working state.

  Workaround: Perform resurrect operation on the PA. Note: this will affect all interfaces on that PA.

IP Routing Protocols

- CSCdr31946

  Symptoms: A Cisco router that is runs Enhanced Interior Gateway Routing Protocol (EIGRP) with the stub feature enabled may have a route that is active and not waiting for replies.

Conditions: This symptom is observed only in networks where all of the EIGRP neighbors are declared as stub.

Workaround: Remove the EIGRP stub feature or clear the IP EIGRP neighbors.

- CSCee28126

  Symptoms: A Cisco router crashes after configuring a sham link, and the sham link endpoints have different area IDs.

  Conditions: This symptom is observed when the areas on the two sham link endpoints are different.

  Workaround: When configuring sham links, be sure that the same area is configured on both endpoints.

- CSCee66936

  Symptoms: A software-forced reload may occur on a router that is configured with a DVMRP tunnel.

  Conditions: This symptom is observed on a Cisco router when the DVMRP tunnel is brought up and routing information is redistributed between DVMRP and MBGP.

  Workaround: There is no workaround.

- CSCef57803

  Symptoms: In a VPNv4 network in which a multi-homed CE router advertises multiple paths for a prefix, a PE router may fail to withdraw the prefix previously advertised to another PE router when its best path changes from a non-imported path to an imported path because of a change in the import route map of the VRF.

  Conditions: This symptom is observed in a topology in which a CE router connects to a PE router via two different VRFs.

  Workaround: Remove the imported path either by unconfiguring the import route map of the VRF or by changing the import route target, withdraw the non-imported prefix from the CE router, and restore the import route map or import route target.

- CSCef92863

  Symptoms: A Cisco 10000 PRE-1 may reload when a VRF that is configured with eight maximum paths is modified.

  Conditions: This symptom is observed when a VRF on the Cisco 10000 series is configured for eight maximum EIBGP paths by entering the **maximum-paths eibgp 8** command and when the VRF is modified in such a way that there is a change in the number of paths that are available. The symptom may also occur on a Cisco 10720.

  Workaround: A Cisco 10000 series can support only six maximum paths. Therefore, configure the number of maximum paths by entering the **maximum-paths eibgp 6** command.

- CSCef93215

  Symptoms: A router that is configured for OSPF may reload unexpectedly and reference the "ospf_build_one_paced_update" process.

  Conditions: This is observed on a Cisco router that has a mixture of LSAs (of type 5 and 11) that travel throughout an autonomous system and LSAs (of any type other than type 5 and 11) that travel within a particular OSPF area. The symptom may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA.

  Workaround: There is no workaround.

Further Problem Description: The symptom is very unlikely to occur. The symptom does not occur on a router that has exclusively stub areas and NSSA areas. The symptom may occur when a router does not have exclusively stub areas and NSSA areas.

- CSCef97738

  Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

  Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

  Workaround: Remove and add the MDT statement in the VRF.

- CSCeg19442

  Symptoms: A router that is configured with the OSPF routing protocol may reload.

  Conditions: This symptom is observed when the OSPF process is simultaneously deconfigured via one session and configured via another session.

  Workaround: There is no workaround. Cisco strongly discourages you to configure a router via two different but simultaneous sessions.

- CSCeg70726

  Symptoms: A router may crash when you enable MVPN by entering the **mdt default** *group-address* command under a VRF.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

  Workaround: There is no workaround.

- CSCsa57101

  Symptoms: A Cisco router may reload when the RSVP MIB object is polled via SNMP.

  Conditions: The symptom is platform- and release-independent.

  Workaround: Disable SNMP by entering the **no snmp-server host** command.

- CSCuk54787

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

ISO CLNS

- CSCeg00610

  Symptoms: A router running Cisco IOS software may reload unexpectedly.

  Conditions: This symptom has occurred when running those versions of software with the Integrated Intermediate System-to-Intermediate System (IS-IS) Incremental shortest path first (SPF) feature and when IS-IS Incremental SPF feature is enabled to run.

  Workaround: Disabled IS-IS Incremental SPF.

- CSCeh17636

  Symptoms: The ISIS metrics assigned to passive-interfaces on a Cisco router will be removed from the configuration after each reload. The passive- interface ISIS metric is used for biasing peer traffic on certain routers.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(28)S1.

  Workaround: Reconfigure the ISIS metric after each reload.

Miscellaneous

- CSCeb84128

  Symptoms: A Cisco 10000 series may stop responding.

  Conditions: This symptom is observed when you attach a child policy map with four policing statements to a parent policy map with a bandwidth queue and when the parent policy map is already attached to 100 T1 interfaces.

  Workaround: Attach the child policy map to the parent policy map before you attach the parent policy map to the interfaces.

- CSCed57204

  Symptoms: When a large number of VRFs are configured, input OAM F5 loopback cells on the ATM interface are dropped continuously, even without traffic. You can see drops at "OAM cell drops" in the output of the **show atm traffic** EXEC command and at "Input queue drops" in the output of the **show interface ATM** EXEC command.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(19), Release 12.3(5), or Release 12.3(4)T2 when the **oam-pvc manage** and **ip vrf** global configuration commands are configured. The symptom may also occur in other releases.

  Workaround: Remove the **ip vrf** command. There is no workaround for a router such as a provider edge (PE) router that cannot remove VRFs.

- CSCee49035

  Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

  Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

  Workaround: There is no workaround.

- CSCee66058

  Symptoms: SNMP users that have MD5 configured may become lost after a switchover in an RPR+ environment.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series that run Cisco IOS Release 12.0(27)S1 in RPR+ mode.

  Workaround: There is no workaround.

- CSCee83781

  Symptoms: A Cisco router may reload when you enter the **show ipv6 mfib verbose** command for a large MFIB.

Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast.

Workaround: There is no workaround.

- CSCef23912

  Symptoms: A traceback is generated on the console and logged in the logging buffer, and the count in the output of the **show alignment** command increments.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured as a provider edge (PE) router when you enter the **show mpls forwarding** command to show the pop labels and the active LDP peers.

  Workaround: There is no workaround.

- CSCef25686

  Symptoms: A number of PVCs may become locked in an inactive state, and the following type of error message may appear in the log:

  ```
  %ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=X, VPI=X, VCI=X) on Interface ATM
  X/X/X, (Cause of the failure: PVC removal during recreation failed)
  ```

  Conditions: This symptom is observed when you change the parameters of a VC class while the PVC is active and while you view the PVC status in the output of the **show atm vc interface** *interface-number command.*

  The symptom occurs when you change the PVC speed in a VC class via one Telnet (or console) session and you enter the **show atm vc interface** *interface-number command via another Telnet (or console) session.*

  Workaround: To remotely resolve the symptoms, remotely initiate an HA failover or remotely reload the affected router.

- CSCef25953

  Symptoms: DSCP-based DWRED statistics are not updated in output of the **show policy-map interface** command: random drop and tail drop statistics are always shown as zero.

  Conditions: This symptom is observed on a Cisco 7500 that is configured with an RSP4. However, this caveat may be platform-independent.

  Workaround: There is no workaround.

- CSCef35911

  Symptoms: MPLS IAS traffic without labels is dropped at one ASBR when PPP encapsulation is configured between two ASBRs.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that functions as an ASBR. However, the symptom may be platform-independent and may also occur in other releases.

  Workaround: Change the encapsulation to HDLC.

- CSCef43691

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages 2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks 3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef63272

  Symptoms: A recursive static default route may not have an outgoing MPLS label, causing all packets to be dropped.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(9) but may also occur in other releases.

  Workaround: Add a nonrecursive static route to the BGP next-hop.

- CSCef67911

  Symptoms: Multicast traffic stops on a PE router that is configured for mVPN.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router when a default MDT switchover to the data MDT occurs.

  Workaround: Clear the VRF mroutes on the affected line card by entering the **clear ip mds vrf** *vrf-name* **forwarding** command.

- CSCef69631

  Symptoms: All line cards may reset and may not enter the “RUN” state after a software OIR or the primary CSC occurs on a Cisco 12000 series that has 40 GB of fabric.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

  Workaround: Power cycle the router.

- CSCef70242

  Symptoms: Low latency queueing (LLQ) and class-based weighted fair queueing (CBWFQ) may not function for MPLS packets. The MPLS packets that conform to the bandwidth that is allocated to these classes may be dropped.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2S when MPLS packets leave an interface that has an output policy map with **priority** or **bandwidth** commands, or both, configured within its classes. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCef70566

  Symptoms: After you have configured an ACL on a router to deny a traffic stream, traffic is shaped unexpectedly.

Conditions: This symptom is observed when the **no access-list** command fails while a nonvolatile generation (NVGEN) occurs.

Workaround: There is no workaround.

- CSCef89470

  Symptoms: After you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an active GE interface or after you reload the router while an GE interface is active, the correct ARP entry is missing from the interface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS release later than Release 12.0(23)S.

  Workaround: There is no workaround.

- CSCef90783

  Symptoms: The output counter on the interface of a PE router that faces a P router generates almost twice the value that is should provide.

  Conditions: This symptom is observed in the following MPLS topology in which Cisco 12000 series routers are connected via interfaces of Engine 3 line cards:

  A CE router (CE1) connects to a PE router (PE1) that connects, in turn, to a P router. This P router connects to another PE router (PE2) that, in turn, connects to another CE (CE2) router.

  The symptom occurs when a VRF ping is generated from PE1 to the VRF interface of PE2, that is, the interface that is connected to CE2. The output counter on PE2 generates incorrect values.

  Workaround: There is no workaround.

- CSCeg03606

  Symptoms: Multicast VPN (MVPN) traffic does not resume.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that functions as a PE router that is configured for MVPN.

  Workaround: Enter the **clear ip mroute** command.

- CSCeg05681

  Symptoms: A CSC OIR may cause all line cards in a router to enter the disabled state and the standby RP to reload continuously.

  Conditions: The symptom is observed on a Cisco 12000 series that has dual PRPs and that runs a Cisco IOS interim release for Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCeg12649

  Symptoms: On a Cisco router that functions as an egress PE router in an MPLS VPN network, after the customer-facing line card is reloaded, the ingress line card that receives an incoming VPN label with a destination with a glean adjacency (which requires an ARP request) without a BGP session may not properly complete the adjacency, causing traffic to be dropped.

  Conditions: This symptom is mostly observed with static recursive route configurations. You can recover from the symptom by manually pinging the interface of the CE router from the adjacent PE router.

  Workaround: Configure static ARP entries for the next hop router in the static recursive routes.

- CSCeg19635

  Symptoms: The PXF engine on a Cisco 10000 series may crash, causing traffic through the router to be interrupted temporarily.

Conditions: This symptom is observed on a Cisco 10000 series when a security ACL is changed and immediately applied to an interface while traffic is traversing the interface. The symptom may occur on a Cisco 10000 series that is configured with either a PRE1 or a PRE2.

Workaround: Wait several seconds between updating the ACL and applying it to the interface.

- CSCeg20771

  Symptoms: During intense interaction between the RP and line cards, the RP may crash because of a corruption. This symptom occurs when large numbers of VRFs are continuously created and deleted. However, the trigger for the symptom to occur could be caused by something else.

  Conditions: This symptom is observed on a Cisco 12410 that is configured with about 100 VRFs and that runs Cisco IOS Release 12.0(27)S2, 12.0(28)S1, or an interim release for Release 12.0(29)S. The symptom is not observed in Release 12.0(30)S.

  Workaround: Do not add or delete more than VRFs at one time.

- CSCeg25493

  Symptoms: Several VIPs may crash at about the same time because of a bus error.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S4 and that is configured with an RSP4 when the VIPs are configured for QoS but have insufficient memory.

  Workaround: Increase the amount of memory on the VIPs.

- CSCeg35517

  Symptoms: An Engine 3 1-port OC-12 channelized DS1 line card that is configured for MLP may reset or may cause the RP to reset.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S.

  Workaround: There is no workaround.

- CSCeg36748

  Symptoms: The **show redundancy** command incorrectly indicates Peer RP is disabled during the upgrade procedure when it is not.

  Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(30)S.

  Workaround: Continue with the upgrade procedure.

- CSCeg37524

  Symptoms: A 4-port OC-12 ATM single mode (4OC12/ATM-IR-SC) line card may generate unicast send timeout errors, %LC-3-PSAERRS errors, and %LC-3-BMAERRS errors, which cause TDP neighbor flapping and may cause the line card to crash.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3.

  Workaround: There is no workaround.

- CSCeg65439

  Symptoms: A Cisco 12000 series may hang while reloading.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz or c12kprp-p-mz image of an interim release for Cisco IOS Release 12.0(31)S.

  Workaround: There is no workaround.

- CSCeg66282

  Symptoms: The controller of a 1-port multichannel STM-1 port adapter (PA-MC-STM1) does not come up after the router has reloaded.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S2.

  Workaround: There is no workaround.

- CSCeg73076

  Symptoms: A Cisco 10000 series reloads when a large QoS policy is defined.

  Conditions: The symptom is observed when you define a policy map that exceeds the number of classes that can be defined in a policy (32).

  Workaround: Avoid policies with an unsupported number of classes.

- CSCeg79456

  Symptoms: An Engine 6 line card may reset because of an IPC timeout.

  Conditions: This symptom is observed on a Cisco 12816 that runs Cisco IOS Release 12.0(27)S4 when you enter the **shutdown** command on the primary Clock Scheduler Card (CSC) or you enter the **no shutdown** command on the secondary CSC that is in the shut down state.

  Workaround: There is no workaround.

- CSCeg83399

  Symptoms: When an ATM PVC is configured with an egress service policy, exiting from the PVC configuration mode by entering the **exit** command, can cause traffic that is forwarded from other PVCs on the line card to be dropped

  Conditions: This symptom is observed on a Cisco 12000 series router with an E3 ATM or E2 8xOC3 ATM line card installed.

  Any action to cause the affected ATM PVC to be reinitialized will restore traffic forwarding.

  Workaround: Do not enter the **exit** command to exit from the PVC configuration mode. Rather, enter **end** command.

- CSCeg88655

  Symptoms: A RP switchover causes %SYS-2-NOTQ and %SYS-2-LINKED errors and some tracebacks on a Cisco 12000 series 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card.

  Conditions: This symptom is observed on a Cisco 12000 series dual-PRP router that runs a Cisco IOS interim release for Release 12.0(31)S.

  Workaround: There is no workaround.

- CSCeg89202

  Symptoms: When you attach a policy with a priority class to a subinterface of a channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c, OC-12c/STM-4c) POS/SDH ISE line card that is configured with Frame Relay subinterfaces, the default queue limit for the priority queue of the port changes to a value that is calculated by the policy map that was attached. This situation causes QoS to be impacted.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: Ensure that the policy map that you attach last calculates the desired queue limit, which is then applied to all subinterfaces of the port.

- CSCeh00169

  Symptoms: After you have reloaded a router, for each of the service policies that are attached to the interfaces of a 4-port OC-12 POS ISE line card, the policing of L2 VCs may fail when errors with the following associated error messages occur:

  ```
  "Must remove existing service policy first .."
  ```

  or

  ```
  "Configured exceed actions are not supported when policing L2 VCs on interface.."
  ```

  When the policing of L2 VCs fails, the following error message is generated:

  ```
  "L2 policing config failed."
  ```

  Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs and 4-port OC-12 POS ISE line card that has a service policy attached to each of its interfaces.

  Following are examples of configurations that may trigger the symptoms:

  ```
  policy-map testing-input
   class class-default
    police cir percent 2 pir percent 4
     conform-action set-mpls-exp-imposition-transmit 4
     exceed-action set-mpls-exp-imposition-transmit 1
     violate-action drop
  !
  map-class frame-relay testing
   service-policy input testing-input

  interface POS6/0
   frame-relay interface-dlci 17 switched
    class testing
  ```

  Workaround: There is no workaround.

- CSCeh02579

  Symptoms: A multilink bundle on a Cisco 10000 series may lock up. The multilink bundle may transmit packets but does not process any incoming packets, indicating that all links of the bundle are in an out-of-order state and draining.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX, Release 12.0(26)S4, or a later 12.0S release and that is configured for mVPN and MLP. The symptom may be platform-independent.

  Workaround: If this is an option, disable mVPN.

- CSCeh05751

  Symptoms: Hardware multicast may be disabled on an Engine 3 line card and the line card may reset.

  Conditions: This symptom is observed when you scale BGP routes and load-balancing on a PE router that is configured for MVPN.

  Workaround: There is no workaround.

- CSCeh07851

  Symptoms: There are several symptoms:

- Multicast traffic may be punted to the RP with the “no group” reason, even if (*,G) and (S,G) exist on the PXF. You can observe the punted traffic in the output of the **show hardware pxf cpu statistics diversion** command.

- PIM neighbors across an MDT in an MVPN network may flap.

Conditions: This symptom is rarely observed when either PXF or the router is rebooted or reloaded while traffic runs in the network. When the router has a large configuration or when many multicast streams pass through the router, the probability of the symptom occurring increases.

Workaround: Make a note of the traffic streams that are punted to the RP by entering the **show hardware pxf cpu statistics spd** command. Then, clear these traffic streams by entering the **clear ip mroute** *group* command.

When the multicast routing table is small, just enter the **clear ip mroute *** command.

Further Problem Description: The packets that are punted to the RP are rate-limited by a multicast data traffic SPD process. These packets are counted as “no group”.

In an MVPN network, control plane traffic is encapsulated in an MDT. If this MDT traffic is punted and rate-limited, the control plane traffic is lost, causing PIM neighbors to flap.

- CSCeh11537

  Symptoms: The PIM neighbor ship on a VRF goes down, preventing traffic from flowing.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for MVPN when you perform one of the following actions:

  - You shut down a line card that is used by MVPN to punt control packets to the RP.

  - You change the VRF name on the line card that is used by MVPN to punt control packets to the RP.

  Workaround: If the symptom occurs because you shut down the line card, re-insert the line card to restore the PIM neighborship. If the symptom occurs because you changed the VRF name on the line card, disable and re-enable the **mdt default** *group-address* command that is defined under the **ip vrf** command.

- CSCeh15364

  Symptoms: On a router that is configured for multi-router APS, the APS interfaces remain in the Active/Inactive states. One of the interfaces is Active, while the other is Inactive. However, when the line card holding the APS protect interface is reloaded and the line card comes back up, both the Working and Protect interfaces end up in Active state.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S2. Not every protect line card reload causes the symptom occur. The symptom is readily observed when the reload of a Protect line card is accompanied by a simultaneously occurring Signal Fail/Signal Degrade (set/clear) event on the Working line card.

  Workaround: There is no workaround to prevent the symptom from occurring. However, when both interfaces are in the Active state, a manual or forced APS switch may restore sanity to the APS states.

- CSCeh17756

  Symptoms: The PIM assert mechanism may not function properly, causing PE routers to remove VRF subinterfaces from output interface lists, and, in turn, causing multicast traffic to be dropped.

  Conditions: This symptom is observed when redundant PE routers and CE routers are located on one LAN segment and when the CE routers select different PE routers as their next hop.

  Workaround: Change the configuration in such a way that all CE routers on one LAN segment select the same PE router as their next hop.

- CSCeh20201

  Symptoms: Traffic entering a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card is dropped.

  Conditions: This symptom is observed on a Cisco 12000 series when an MLP interface is moved from the 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card to another line card.

  Workaround: There is no workaround.

- CSCeh20219

  Symptoms: The policer does not function for nxDs0 interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured with a 1-port channelized OC-12c/STM-4 (DS1/E1) ISE line card.

  Workaround: There is no workaround.

- CSCeh27734

  Symptoms: For recursive routes with implicit null as the local label, the FIB may point to the rewrite of the parent prefix. However, this situation may not affect any functionality.

  Conditions: This symptom is observed on a router that is configured for MPLS forwarding.

  Workaround: Change the affected prefix to be non-recursive.

- CSCeh31939

  Symptoms: When a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card is configured for MVPN on MLP interfaces and you reload the router, the PIM VRF neighbor may not be established via a tunnel for some MLP interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(31)S.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MLP interfaces.

- CSCeh33574

  Symptoms: An Engine 4 plus or Engine 5 line card does not come up.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S when IPC timeout errors occur.

  Workaround: There is no workaround.

- CSCeh34989

  Symptoms: One of the following two symptoms may occur on a POS ISE egress line card:

  – The interface may become stuck during transmission. The line protocol will continuously flap because the interface continues to receive keepalives but is not able to send any keepalives.

  – The line card generates the following harmless error message:

  ```
  %EE48-4-GULF_TX_SRAM_ERROR: ASIC GULF: TX bad packet header detected.
  Details=0x4000
  ```

  Conditions: These symptoms are observed on a Cisco 12000 series when an invalid packet is forwarded to an egress interface on an ISE line card.

  Workaround: If the transmission on the interface is stuck, reload the line card by entering the **hw-module slot** *x* **reload** command.

- CSCeh36824

Symptoms: When the HA mode is RPR+ and a standby PRE comes up after a crash, the HA mode may change from RPR+ to SSO and the standby PRE displays error messages that indicate that the running configuration of the active PRE is "mode rpr-plus" but the running configuration of the standby PRE is "mode sso."

When the HA mode is SSO and a standby PRE comes up after a crash, the standby PRE may become stuck in its initialization and does not enter the "STANDBY_HOT" state.

Conditions: These symptoms are observed on a Cisco 10000 series when the standby PRE crashes but does not report a switchover (that is, a "standby down" event occurs but not a switchover event), causing the standby PRE to come up in an inconsistent state. When the standby PRE crashes, the active PRE shows an error message that includes the text "PEER_CRASH_INTERRUPT."

Workaround: Reset the standby PRE by entering the **hw-modulestandby-cpu reset** command to enable it to reload and come back up properly.

- CSCeh37351

  Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

  - tag2ip, with bad ip hdr cksum
  - tag2ip, with ip->tl > L2
  - tag2ip, with ip->tl < 20
  - tag2ip, with ip options packets
  - tag2ip, with ip options packets with bad ip hdr cksum
  - tag2ip, with ip options packets with ip->tl > L2
  - tag2ip, with ip options packets with ip->tl < 20

  These bad packets cause packet corruption and an "TX192-3-PAM_PIM" error message on the E4+ line card and may even cause the E4+ line card to reset.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh40882

  Symptoms: On a Cisco 12000 series router with a 1xChOC12/DS1 ISE line card configured with multilink MFR protocol and a MQC policy, after a reload the QoS does not get applied to the bundle. The QoS goes to the suspend mode.

  Conditions: The bundle loses its QoS policy when the router is reloaded. This problem is observed when running Cisco IOS Releases 12.0(28)S1, 12.0(30)S, and an interim release for Release 12.0(31)S.

  Workaround: Remove the service-policy from the bundle and re-apply it.

- CSCeh42465

  Symptoms: An Engine 3 line card sends unlabeled traffic after it has been toggled from explicit routing to default routing. The symptom is related to the handling of a default-route on an Engine 3 ingress line card that functions in an IP-to-MPLS path.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 or any other image that includes the fix for caveat CSCsa64782, which is a preliminary requisite for default-route handling on an Engine 3 line card. The symptom occurs in the following scenario:

1) You configure BGP to advertise the target address, so the target address is directly known in the routing table.

2) You remove the advertisement from BGP and return to default routing, with the same source for the next hop as the platform that was the BGP next hop.

3) You enter the **clear ip route** *network* command, with the address of the BGP next hop for the *network* argument.

After the transition from non-default routing to default routing, entering the **clear ip route** *network* command, with the address of the next hop for the *network* argument, causes an inconsistency, and traffic is forwarded as unlabeled.

Workaround: To restore proper operation, enter the **clear ip route 0.0.0.0** command.

- CSCin75746

  Symptoms: When you perform an OIR of a PA-MC-8TE1 port adapter or you reload microcode onto the line card, the line card may generate the following error message and may stop forwarding traffic:

  AC Switching: VIP Xmit failed: DLCI 426 context missing

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: There is no workaround. To re-enable the line card, enter the **tx-queue-limit** command on the affected interface of the line card.

- CSCin87776

  Symptoms: Multilink bundles on a Cisco 7500 series may process-switch traffic instead of using dCEF, causing the CPU usage of the RSP to increase sharply and a CPU hog condition to occur.

  Conditions: This symptom is observed when an RPR+ switchover occurs on a Cisco 7500 series that is configured for HA.(The switchover causes an MLP to flap.) However, the symptom may also occur on a Cisco 7500 series that has a single RP (so, without a switchover) when an MLP link flaps.

  Workaround: There is no workaround. Note that the symptom does not occur when SSO is configured because the MLP state is maintained.

- CSCin88026

  Symptoms: A VIP that is configured for Link Fragmentation and Interleaving may crash during the "vip_mlp_process_reassemble" process.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS interim release for Release 12.0(31)S when links flaps occur on the port adapter that is installed in the VIP while traffic is being processed.

  Workaround: There is no workaround.

- CSCin88273

  Symptoms: After an RPR+ or SSO switchover occurs, an MLP sequence number mismatch may occur, a ping between back-to-back interfaces may not go through, and the routing protocol through this link may go down.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dMLP and RPR+ or SSO.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the multilink interface of the Cisco 7500 series.

- CSCin88303

  Symptoms: The line protocol of unchannelized interfaces on a PA-MC-2T3+ port adaptor remains down although the link is up.

  Conditions: This is observed when you change from the channelized mode to the unchannelized mode by entering the **no channelized** command on the T3 controller of the PA-MC-2T3+ port adaptor.

  Workaround: There is no workaround.

- CSCin88356

  Symptoms: The output of the **show interfaces serial** *number* command does not show the total output packet drops.

  Conditions: This symptom is observed when you apply a service policy on an interface that is configured for CEF.

  Workaround: Enter the **show policy map interface** *interface-name* command to see the total output packet drops.

- CSCin88417

  Symptoms: Transmit accumulator loss may occur for MLP interfaces after you have performed an OIR of a VIP. When the transmit accumulator value goes to zero, MLP may stop forwarding or packets may be switched by dCEF.

  Conditions: This symptom is observed after you have performed an OIR of a VIP while traffic is running on MLP bundles.

  Workaround: Reload the VIP again and ensure that no traffic leaves from the MLP bundles immediately after the VIP comes up.

- CSCin89330

  Symptoms: Distributed MFR does not function, that is, a ping on a distributed MFR interface fails.

  Conditions: This symptom is observed on a Cisco 7500 series that has a distributed MFR interface.

  Workaround: There is no workaround.

- CSCsa41907

  Symptoms: When a channel group is removed from and added to a controller and when a PRE switchover occurs, the line protocol on another channel goes down after a while and input packets are not counted.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 6-port channelized T3 line card.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

  Alternate Workaround: Ensure that the you enter the **hw-module standby-cpu reset** command before a PRE switchover occurs.

- CSCsa42857

  Symptoms: A duplex configuration (half/full) is not saved to NVRAM. This situation causes the default configuration (half duplex) to be used after the router reloads.

  Conditions: This symptom is observed on a PA-2FE port adapter that is installed in a Cisco 7200 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: There is no workaround.

- CSCsa46699

  Symptoms: A Cisco 7200 series may crash because of a bus error when you remove a subinterface or when you remove a service policy from an interface.

  Conditions: This symptom is observed when a hierarchical policy map is configured, when the policy map has a police action in the child only, and when the policy map is attached to two interfaces. When the service policy is removed from one of the interfaces, the router may crash.

  Workaround: Configure the same policy map with a different name on each interface.

- CSCsa46859

  Symptoms: Cisco 10000 series routers using ATM VC bundles and QoS may have packets dropped when an external ATM VC bundle using DSCP type of service traverses the Cisco 10000.

  Conditions: When using ATM VC bundles and Cisco IOS Release 12.0 S on a Cisco 10000 series router, ATM VC bundle traffic may be dropped. The problem arises when ATM bundles using DSCP enter the Cisco 10000 router which only supports MPLS EXP type of service bits. Those code points not matching an MPLS EXP TOS value exactly are dropped.

  Workaround: Either use MPLS EXP for ATM bundles leading into the Cisco 10000 router or only use DSCP values that map to the MPLS EXP values.

- CSCsa46887

  Symptoms: A router builds an Echo Reply that is invalid and may be misunderstood.

  Conditions: This symptom is observed on a router that is configured for LSPV when the router receives an Echo Request with a Pad TLV that has a value of “Copy Pad TLV to reply.” The Echo Reply that the router builds includes residual data from previously received packets instead of the pad pattern that was received.

  Workaround: There is no workaround.

- CSCsa47020

  Symptoms: When Multilink Frame Relay (FRF.16) is configured on two bundled serial links and when the traffic rate is above 2 Mbps, packet loss occurs.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7500 series when you send a 64-byte Ethernet frame. The symptom does not occur when the frame size is 512 bytes or more.

  Workaround: There is no workaround.

- CSCsa49740

  Symptoms: Packets are punted to the GRP at a rate of 5000 pps, causing the CPU utilization of the CPU to reach more than 50 percent.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 when a 4-port Packet-over-SONET OC-48c Engine 4 plus line card (4OC48E/POS-SR-SC=) receives TCP packets with destination 0.0.0.0.

  Workaround: There is no workaround.

- CSCsa53001

  Symptoms: A VIP6-80 in which a PA-MC-STM-1SMI is installed crashes.

  Conditions: This symptom is observed on a Cisco 7500 series that runs a Cisco IOS interim release for Release 12.0(31)S after link flaps occur on the PA-MC-STM-1SMI that has QoS configured its serial interfaces.

Workaround: There is no workaround.

- CSCsa53685

  Symptoms: Incorrect VC12 defect information may be generated on a Cisco 7500 series that is configured with a PA-MC-STM-1.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S1.

  Workaround: There is no workaround.

- CSCsa54891

  Symptoms: Under normal operation, an Engine 6 line card may reset with the following error messages and tracebacks:

```
%TX192-3-CPUIF: Error=0x10
rd 0x73 base 0x73 hdr 0x75 last 0x75 wr 0x75
insert 0x0 back 0x0 len 0x2474 cnt 0x0
-Traceback= 40D89758 405A9008 405EC67C 406D5E7C 406D64F8 400FC020 %TX192-3-CPUIF_ERR:
FIFO RAM3 Parity Error.
-Traceback= 40D89808 405A9008 405EC67C 406D5E7C 406D64F8 400FC020 %GSR-3-INTPROC:
Process Traceback= 400FFD20 400FCAA0 40010F6C
-Traceback= 404EFBCC 406D6760 400FC020
%FABRIC-3-ERR_HANDLE: Due to FIA HALT error, reconfigure FIA on slot 9
```

  Conditions: This symptom is observed on a Cisco 12000 series when false RAM parity errors occur.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat determines whether the RAM parity errors are real or false.

- CSCsa56415

  Symptoms: A router may pause indefinitely or reload unexpectedly.

  Conditions: This symptom is observed while deleting or recreating policing access control lists (ACLs) or shaping ACLs via a script.

  Workaround: Update the access control list (ACL) rather than delete it.

- CSCsa58340

  Symptoms: Upon entering the **police** command, the router reloads unexpectedly.

  Conditions: The reload occurs if the policy map being edited already contains the maximum number of classes that the Cisco 10000 supports and the user attempts to add one more class with police.

  Workaround: Avoid using policy maps that contain more classes than what the Cisco 10000 supports.

- CSCsa59002

  Symptoms: IP fragments with a User Datagram Protocol (UDP) protocol identifier may be improperly denied on an Engine 3 line card that has an outbound access control list (ACL) that denies specific UDP ports.

  Conditions: This symptom is observed only for outbound ACLs on an Engine 3 line card on a Cisco 12000 series. The following is an example of an ACL statement for which the symptom may occur:

```
access-list 100 deny udp any any eq 0 <<< this line may accidently deny IP fragments
for UDP access-list 100 permit ip any any
```

Workaround: Use the following ACL instead of the above-mentioned example:

```
access-list 101 permit udp any any fragments
access-list 101 deny udp any any eq 0
access-list 101 permit ip any any
```

- CSCsa64782

  Symptoms: When an ingress ISE line card is used with a default route that iBGP learns over a MPLS core, the following two symptoms may occur:

  – The output of the **show controllers tofab alpha mip stat | i MTU** command may show traffic drops.

  – Traffic is incorrectly sent as "unlabeled" over the MPLS core.

  Conditions: These symptoms are observed on a Cisco 12000 series when the traffic path follows a recursive default route and when recursive load sharing occurs.

  Workaround: Prevent outbound load sharing to the default route by changing the IGP metrics.

- CSCsa68301

  Symptoms: Inter-MVPN traffic does not function on an Engine 4+ line card.

  Conditions: This symptom is observed on a Cisco 12000 series and may occur with any Engine 4+ line card.

  Workaround: There is no workaround.

- CSCsa68616

  Symptoms: An IPC failure occurs and an OC-12 line card that is configured for Frame Relay over MPLS resets.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

  Workaround: There is no workaround.

  Further Problem Description: The IPC failure and the line card reset occur after a depletion of the elements in the FrFab 608 byte queue for the line card. Consecutive outputs of the **show controllers** *slot-number* **frfab queue** command show a consistent and rapid leak of these buffers.

- CSCsa70274

  Symptoms: A Cisco router may crash during an LSP traceroute when a transit router responds with a downstream map TLV that contains a multipath length field that is set to 0, 1, 2, or 3.

  Conditions: This symptom is observed during testing of the Cisco LSP ping draft version 3 in a network that uses a later version of the LSP ping draft.

  The implementation of draft version 3 does not handle the multipath length field settings correctly. In draft version 3 and earlier drafts, there is an ambiguity on whether or not the multipath length field includes the four bytes comprising of the hash-key type, depth limit, and multipath length fields. As such, all implementations of the draft version 3 encode the length as four bytes and reply with a multipath length of four bytes.

  When an LSP traceroute is invoked and a transit router replies with a downstream map TLV that contains a multipath length field that is set to a length shorter than four bytes, existing implementations handle this situation incorrectly and cause memory packet memory to become corrupted during the subsequent attempt to build an MPLS echo request packet. This situation eventually causes the router to crash.

  Workaround: If LSP traceroute implementations exist on a transit router that cause the transit router to reply with a multipath length that is set to a value other than four, avoid using an LSP traceroute.

Note, however, that the implementations of Cisco LSP ping draft version 3 do not reply with multipath lengths that can cause this crash.

- CSCuk50159

  Symptoms: If CEF is disabled before a switchover is performed, configuring DCEF after the switchover will not enable DCEF on the VIPs.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.0S and that is configured for High Availability.

  Workaround: Make sure that DCEF is running before the switchover.

TCP/IP Host-Mode Services

- CSCeg20351

  Symptoms: An RR is unable to negotiate the optimal MSS with their MP-BGP neighbors.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(28)S1, that functions as an RR, and that has Path MTU Discovery (PMTUD) enabled. The symptom may also occur in other releases.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCef68547

  Symptoms: FR links on 6-port channelized T3 and 2-port OC-3-channelized-to-DS1/E1 line cards may not recover when all of the links are removed and reconfigured for an MFR bundle. The same symptom may occur on serial interfaces.

  Conditions: This symptom is observed when all links are removed from and re-added to the bundle while the bundle is briefly in a shut down state.

  Workaround: To re-establish the bundles, enter the **hw-module slot** *shelf-id/slot-number* **reload** command. You can also delete and reconfigure the MFR interface or the serial interfaces. To prevent the symptom from occurring, wait a couple of seconds between entering the **shutdown** command and the **no shutdown** command when you remove and reconfigure the MFR bundle or serial interfaces.

- CSCeh33185

  Symptoms: On a POS interface on a VIP4-80 that is running PPP, the interface goes down and remains down. A manual shut and no shut of the interface is required to bring it up.

  Conditions: This symptom is observed on a Cisco 7513 RSP that is running Cisco IOS Release 12.0S.

  Workaround: Enter the **shut** command and followed by the **no shut** command on the interface.

- CSCsa49019

  Symptoms: A memory leak may occur in the “Multilink Events” process, which can be seen in the output of the **show memory summary** command:

  0x60BC47D0 0000000024 0000000157 0000003768 MLP bundle name
  0x60BC47D0 0000000028 0000000003 0000000084 MLP bundle name
  0x60BC47D0 0000000044 0000000001 0000000044 MLP bundle name
  0x60BC47D0 0000000048 0000000001 0000000048 MLP bundle name
  0x60BC47D0 0000000060 0000000001 0000000060 MLP bundle name

0x60BC47D0 0000000064 0000000013 0000000832 MLP bundle name
0x60BC47D0 0000000068 0000000008 0000000544 MLP bundle name
0x60BC47D0 0000000072 0000000001 0000000072 MLP bundle name
0x60BC47D0 0000000076 0000000001 0000000076 MLP bundle name
0x60BC47D0 0000000088 0000000018 0000001584 MLP bundle name

Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(28)S2

Cisco IOS Release 12.0(28)S2 is a rebuild of Cisco IOS Release 12.0(28)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(28)S2 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCed64664

  Symptoms: A "%SYS-2-LINKED: Bad enqueue ....." error message may be seen in the syslog of an LNS right after traffic is sent through a PPP multilink bundle that is established via an L2TP session on the LNS. This message is also seen when multilink PPP fragments are switched or when multicast packets are replicated.

  Certain packet buffers (particle clones) are eventually depleted, and multilink fragmentation stops working when all particle clones are exhausted. You can monitor the availability of particle clones by entering the **show buffers | begin Particle Clones:** EXEC command; the command does not produce any output if no more particle clones are available.

  Conditions: This symptom is observed with all features that use particles. The symptom is not specific to VPDN, GRE, or other features that use particles.

  Workaround: There is no workaround.

  Further Problem Description: Different symptoms may occur with different features.

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCed67358

  Symptoms: An IPv6 PIM neighbor may be down after changing the PIM configuration.

Conditions: This symptom is observed when the **no ipv6 pim** command is entered on some subinterfaces of a physical Ethernet interface and when PIM is enabled on several subinterfaces of the same physical Ethernet interface. The symptom affects both IPv4 and IPv6, and configurations with multicast and OSPF Hello messages.

Workaround: There is no workaround.

- CSCee04316

  Symptoms: A TN-2-BADCONN message may appear in the log and may be quickly followed by an FIB Disable message, indicating that distributed CEF is disabled on all VIPs. The IPC buffers usage may grows very large (up to 600 MB) and these buffers may not be reclaimed.

  Conditions: This symptom is observed on a distributed Cisco platform that uses IPC communication with a central route processor and distributed cards when commands are executed on the card (for example, the **execute-on** command, the **show controller vip** command, or other commands) and when the Telnet connection is lost before the execution of the command has completed.

  Workaround: Reload the router to restore normal operation. Review operational monitoring processes and avoid scripts that collect information from the cards.

- CSCee87891

  Symptoms: SNMP entries may be deleted when you configure SNMP or when you reload the router on which SNMP is configured.

  Conditions: This symptom is observed when an SNMP user is configured with the same name or host name as a community.

  Workaround: There is no workaround.

- CSCee95282

  Symptoms: A router may generate a very large remote processing time report that may take between 10 and 25 seconds to be generated.

  Conditions: This symptom is observed when you enter the **rtr responder** command for the first time and you do not reload the router.

  Workaround: Reload the router after you have entered the **rtr responder** command.

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml.

- CSCef53395

  Symptoms: A memory leak may occur in the IPC buffers of a Cisco router, and the output of the **show processes memory** command shows that the Pool Manager process holds increasingly more memory.

```
Router#show proc mem
Total: 231201504, Used: 202492916, Free: 28708588
 PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
...
   5   0  149227592   69514888   79894996  135335724   66834832 Pool Manager
```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S2 or 12.0(26)S3. The memory leak is triggered by the SNMP polling of specific OIDs within the ciscoEnhancedMemPoolMIB MIB.

  Workaround: Prevent the ciscoEnhancedMemPoolMIB MIB from being polled by explicitly configuring an SNMP view. To prevent this MIB from being accessed via any community strings, create a view and apply the view to all communities configured, as in the following example:

```
snmp-server view NOMEMPOOL iso included
snmp-server view NOMEMPOOL ciscoEnhancedMemPoolMIB excluded
snmp-server community public1 view NOMEMPOOL ro 6
snmp-server community public2 view NOMEMPOOL ro 7
snmp-server community public3 view NOMEMPOOL ro 8
```

  The specific MIB that is being blocked is ciscoEnhancedMemPoolMIB (1.3.6.1.4.1.9.9.221).

  Once the configuration is in place, the router must be reloaded to clear the IPC cache and free the memory.

- CSCeg50224

  Symptoms: A standby PRE may crash because of an SNMP set operation during an SSO switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(28)S1. The symptom may be platform-independent.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCef79968

  Symptoms: When an snmpget is executed for an interface index below .1.3.6.1.2.1.31.1.1.1.6, the router responds with the following information:

```
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.12 : VARBIND EXCEPTION: No Such
Instance
```

  However, an snmpwalk executes successfully for an interface index below .1.3.6.1.2.1.31.1.1.1.6.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 when an snmpget is executed for 4GE-SFP-LC subinterfaces or for a 4GE-SFP-LC interface when there is another interface index for the same interface. The symptom may be platform-independent.

  Workaround: Reload the router.

IP Routing Protocols

- CSCea59206

  Symptoms: When you configure the **distribute-list** router configuration command under the **address-family ipv4 vrf** *vrf name* router configuration command, the **distribute-list** router configuration command may appear under the main routing process as may be displayed in the output of the **show running-config** EXEC command.

  Conditions: This symptom is observed in either a Routing Information Protocol version 2 (RIPv2) or a Border Gateway Protocol (BGP) configuration when you specify the *interface-type* and *interface-number* arguments of the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} [*interface-type interface-number*] router configuration command.

  The symptom does not occur when you do not define the *interface-type* and *interface-number* arguments and only enter the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} router configuration command.

  Workaround: There is no workaround.

- CSCec22723

  Symptoms: A router may unexpectedly reload because of a watchdog timeout or bus error in OSPF.

  Conditions: This symptom is observed when iSPF is configured under OSPF.

  Workaround: Remove the iSPF configuration from OSPF by entering the **no ispf** command.

- CSCed93804

  Symptoms: EIGRP may incorrectly remove a connected route from a topology.

  Conditions: This symptom is observed when you change the router network commands and there are overlapping networks. For example, if the following is configured:

  ```
  int loopback1
     ip addr 10.1.2.2 255.255.255.0
  router eigrp 1
     net 10.0.0.0 0.3.255.255
  ```

  and you change the network command to:

  ```
  router(config-router)# net 10.0.0.0
  router(config-router)# no net 10.0.0.0 0.3.255.255
  ```

  the connected route will be removed when it should be retained.

  Workaround: Remove the old network command first before adding the new one, for example:

  ```
  router(config-router)# no net 10.0.0.0 0.3.255.255
  router(config-router)# net 10.0.0.0
  ```

- CSCee28148

  Symptoms: After a switchover on a router, one or more obsolete LSAs from a neighboring router may still be present in the topology. This is improper behavior: the LSAs should no longer be present in the topology.

  Conditions: This symptom is observed when a switchover occur on a Cisco router that runs OSPF NSF and when a neighboring router flushes one or more of its self-originated LSAs.

  Note that the LSAs automatically age out within an hour, unless the link that connects the router and the neighboring router is a demand circuit or has OSPF “flood-reduction” configured.

Workaround: If the LSA is an external LSA (type5/type7), enter the **clear ip ospf redistribution** command on the neighboring router. In all other cases, enter the **clear ip ospf process** command on the neighboring router.

- CSCee67164

  Symptoms: A router LSA is not generated for a loopback address.

  Conditions: This symptom is observed when you assign an IP address to an unnumbered interface.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the loopback interface.

- CSCee85676

  Symptoms: When VPNv4 route advertisement are received after BGP has converged, the existing path is updated but imported paths from the original path are not updated accordingly.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the **maximum-paths** *number-of-paths* **import** *number-of-paths* command is enabled. The symptom occurs when the path attributes are changed dynamically instead of the path being completely withdrawn and readvertised.

  Workaround: Withdraw the prefix from the remote PE router and then readvertise the prefix.

- CSCee86530

  Symptoms: A BGP update that is sent to a connected P router fails to report the martian next-hop log message when the next-hop field in the attribute of the BGP update is set to 255.255.255.255 (that is, all 1's). The P router does deny the advertisement of the MP_REACH_NLRI attribute to the other PE routers, but there is no log message to indicate that it is denying the advertisement and why it does so.

  Conditions: This symptom is observed during MP-BGP negative testing for the MP_REACH attribute.

  Workaround: There is no workaround.

- CSCee88542

  Symptoms: A Cisco router may reload unexpectedly when you enter the **show ip msdp peer** command.

  Conditions: This symptom is observed when the MSDP session flaps while you enter the **show ip msdp peer** command.

  Workaround: There is no workaround.

- CSCef91275

  Symptoms: An MPLS TE tunnel stays stuck in the "Path Half Admitting" state, as is shown by the output of the **show mpls traffic-eng tunnel** command, thereby preventing the tunnel from coming up.

  Conditions: This symptom may be observed when a particular third-party router that functions as the headend for the MPLS TE tunnel sends a Path message to a Cisco router that functions as the midpoint for the router MPLS TE tunnel and that does not have the **mpls traffic-eng tunnels** interface configuration command enabled on the outbound interface that would be used to forward the Path message.

  Workaround: Enter the **mpls traffic-eng tunnels** interface configuration command on the outbound interface of the Cisco router. Then, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on this interface, and save the configuration.

Miscellaneous

- CSCeb52181

  Symptoms: A Cisco platform that accesses the “system:/vfiles/tmstats_ascii” virtual file (for example, via “more system:/vfiles/tmstats_ascii”) may crash because of bus error.

  Conditions: This symptom is observed under normal working conditions when no configuration changes are made on a Cisco platform that runs Cisco IOS Release 12.0 S, 12.1 E, 12.2 or 12.3. When the “system:/vfiles/tmstats_ascii” virtual file is not used, the symptom does not occur.

  Workaround: There is no workaround.

- CSCed20839

  Symptoms: After an interface flaps or when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface that is configured for Hot Standby Router Protocol (HSRP), a virtual HSRP address may not respond to pings.

  Conditions: This symptom is observed on a Cisco router that is configured with a 2-port Fast Ethernet Inter-Switch Link (ISL) port adapter (PA-2FEISL) that has at least one Fast Ethernet interface configured for HSRP.

  The symptom occurs because the Fast Ethernet interface that is configured for HSRP is not switched to promiscuous mode when the HSRP group becomes active, preventing packets that are addressed to the HSRP virtual MAC address from being received by the interface. The output of the **show controllers fastethernet** user EXEC or privileged EXEC command displays whether the promiscuous mode is enabled or disabled.

  Reboot the router to restore the router to proper operation.

  Workaround: To prevent the symptom from occurring, enter the **standby use-bia** interface configuration command on the Fast Ethernet interface that is configured for HSRP.

  Further Problem Description: This caveat only effects Fast Ethernet port adapters and network modules that use the AMDP2 chipset (for example, the PA-2FEISL). When you use such a port adapter or network module with HSRP configured and the interface goes down, HSRP does no longer function when the interface comes back up.

- CSCed47560

  Symptoms: The native Gigabit Ethernet ports of a Cisco 7200 series NPE-G1 or a Cisco 7301 may stop forwarding traffic.

  Conditions: This symptom is observed in a stress situation when bursty traffic is received.

  Workaround: There is no workaround.

- CSCed79218

  Symptoms: A Cisco 7200 series router with a PA-2CT3+ or PA-CT3 port adapter does not provide the configured minimum bandwidth guarantees.

  Conditions: This behavior appears to be limited to the multichannel T3 family of port adapters and appears consistently upon the configuration of CBWFQ.

  Workaround: There is no workaround.

- CSCed81317

  Symptoms: When an import map is configured on a VPN Routing/Forwarding (VRF) instance, the CE-learned routes are filtered out, preventing them from appearing in the VRF routing table.

Conditions: This symptom is observed when the **import map** *word* command is configured as part of the VRF configuration. Note that eBGP routes are not filtered out.

Workaround: There is no workaround.

- CSCed85254

  Symptoms: MPLS forwarding may stop.

  Conditions: This symptom is observed under the following conditions:

  - When you change a COS map or prefix map.
  - When you change an IP access list.

  Workaround: There is no workaround.

- CSCed85324

  Symptoms: Stale MPLS COS per-route entries may be left behind.

  Conditions: This symptom is observed after the route disappears from the routing table in cell mode multi-VC network.

  Workaround: There is no workaround.

- CSCed95499

  Symptoms: A Cisco router may crash if a PA driver attempts to convert an uncached iomem address to a cached iomem address.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

- CSCee07351

  Symptoms: An LC-ATM-enabled subinterface on a PE router remains in the "not ready" state when you view the LDP session to the LSC in the output of the **show mpls ldp discovery** command. Entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on either the LC-ATM subinterface on the PE router or on the Xtag interface on the connected LSC does not clear the problem.

  Conditions: This symptom is observed when the interface stays in the "interface not LDP ready" state and when there exists a stray LVC on the switch interface. The PE router reaches this state after multiple LDP flaps.

  Workaround: Clear the symptoms by entering the **clear ip route** *prefix* command, in which the *prefix* argument is the local loopback address for the LC-ATM subinterface. Doing so causes all tailend LVCs on all LC-ATM subinterfaces to be torn down and re-established, and causes a brief customer outage. Only use this workaround if no alternate path (such as a redundant LC-ATM subinterface) exists for MPLS traffic towards the device. After applying the workaround, check the output of the **show mpls atm summary** command to confirm that the expected number of LVCs has been re-established. If bindings are not successfully re-established, re-enter the **clear ip route** *prefix* command, or reload the router.

  When you reload the router, the stray LVC is removed and the LDP session on the LC-ATM subinterface of the PE router is brought back to a normal state.

- CSCee16205

  Symptoms: The committed information rate (CIR), normal burst, and maximum burst of the **police** (percent) command in a policy map are set incorrectly.

  Conditions: This symptom is observed when the policy map is attached to an MLP interface that is configured for LFI and that is in the "DOWN" state.

Workaround: Attach the policy map when the MLP interface is in the “UP” state.

- CSCee18883

  Symptoms: All VIPs in a Cisco 7500 series restart as a consequence of a Cbus complex that is triggered by a stuck output. Just before the output becomes stuck, IPC timeout errors occur.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(5) in a dLFIoATM environment. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee31196

  Symptoms: An LDP session over a tunnel interface may drop and not come back up.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.0(27)S1 when auto-tunnel traffic engineering is configured and when RSVP label distribution is configured in the MPLS core.

  Workaround: Run LDP in the MPLS core for all interfaces that have auto-tunnel traffic engineering configured.

- CSCee32365

  Symptoms: When a single bundle link associated with a Multilink Frame Relay (MFR) interface is brought up, LMI exchanges over the MFR interfaces may not happen.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for MFR.

  Workaround: There is no workaround.

- CSCee34622

  Symptoms: Neighbor adjacencies for the IS-IS, OSPF, or other routing protocol may bounce during a Nonstop Forwarding (NSF) switchover.

  Conditions: This symptom is observed when you enable a routing protocol for NSF and you enter the **external overload signalling** router configuration command. The following configuration illustrates this situation for IS-IS:

  router isis *area-tag* **nsf [cisco | ietf] external overload signalling**

  Workaround: Disable the **external overload signalling** router configuration command.

- CSCee49862

  Symptoms: A Cisco 7500 series multichannel T3 port adapter (PA-MC-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCee49983

  Symptoms: When the controller of multichannel T3 port adaptor (PA-MC-2T3+) goes down for a short duration and an alarm occurs, the port adapter does not report the type of alarm.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that are configured with a PA-MC-2T3+. The port adapter should provide a history table of recent alarm conditions along with a corresponding time stamp to allow for proper troubleshooting.

  Workaround: There is no workaround.

- CSCee53461

  Symptoms: BGP adjacencies may time out on an Engine 3 channelized OC-12 line card.

Conditions: This symptom is observed on a Cisco 12000 series when you use Multilink PPP (MLP) interfaces with service policies attached.

Workaround: There is no workaround.

- CSCee53667

  Symptoms: A ping to an interface of an Engine 3 Gigabit Ethernet line card fails after an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series that functions in SSO HA mode when an RP switchover occurs after the line card has been reloaded.

  Workaround: There is no workaround.

- CSCee67278

  Symptoms: A VIP may crash with a bus error and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  This occurs after the following scheduler error in the “req_proc” process:

  ```
  %SYS-2-INTSCHED: ’sleep for’ at level 2 -
  Process= "req_proc", ipl= 2, pid= 27
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs a Cisco IOS image that contains the fix for CSCec07487 when a PA-MC-8TE1+ is installed in the VIP.

  Workaround: There is no workaround.

- CSCee67746

  Symptoms: An E4+ POS line card reports %TX192-3-PAM_MODULE and %TX192-3-PAM_PIM errors. On rare occasions the line card may crash when it receives a malformed packet.

  Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S3 or Release 12.0(26)S4.

  Workaround: There is no workaround.

- CSCee70591

  Symptoms: A Cisco 7500 series T3 port adapter (PA-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCee71156

  Symptoms: Unexpected behavior may occur when the **tx-ring-limit** *ring-limit* command and HQF are configured: a memory leak may occur in the pool manager of the router.

  Conditions: This symptom is observed when traffic is sent at high speed (higher than the line rate) and when the *ring-limit* argument is less than 255.

  Workaround: There is no workaround.

- CSCee72906

  Symptoms: A VIP may crash when you remove a service policy from a multilink interface or when a member link is removed from the multilink interface while heavy traffic is being processed.

  Conditions: This symptom is observed on a Cisco 7500 series that has an RSP and that is configured for dLFI over a leased line, MLP, and QoS.

  Workaround: There is no workaround.

- CSCee79728

  Symptoms: A Cisco 7200 series that operates in the process switching path may crash with a bus error exception.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(13b)M2 and that is configured with a serial or POS port adapter. The symptom may also occur in other releases.

  Workaround: Enter the **ip route cache** command for all interfaces.

- CSCee81490

  Symptoms: MALLOCFAIL messages may be generated during an attempt to allocate large negative and positive memory blocks in the "cpf_process_ipcQ" process:

```
%SYS-2-MALLOCFAIL: Memory allocation of -1622998781 bytes failed from 0x60B5BE48,
alignment 0
Pool: Processor  Free: 371055532  Cause: Not enough free memory
Alternate Pool: None Free: 0  Cause: No Alternate pool
-Process= "cpf_process_ipcQ", ipl= 0, pid= 141
-Traceback= 603DDCB0 603E005C 60B5BE50 60B5C140 60B5C62C 60B59A0C 603D5D1C 603D5D08
```

```
%SYS-2-MALLOCFAIL: Memory allocation of 344820739 bytes failed from 0x60B5BE48,
alignment 0
Pool: Processor  Free: 363937412  Cause: Memory fragmentation
Alternate Pool: None Free: 0  Cause: No Alternate pool
-Process= "cpf_process_ipcQ", ipl= 0, pid= 141
-Traceback= 603DDCB0 603E005C 60B5BE50 60B5C140 60B5C62C 60B59A0C 603D5D1C 603D5D08
```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(24)S5.

- CSCee82681

  Symptoms: On an RTR probe, an RSP does not report input or output packets for serial interfaces of PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2(23a) or Release 12.3 and is more likely to occur when the number of channelized port adapters (such as the PA-MC-8T1, PA-MC-8E1, and PA-MC-8TE1+ port adapters) that are installed in the router is high. The symptom may also occur in other releases.

  Workaround: Reload the router.

  Alternate Workaround: Enter the **reload microcode** router configuration command.

- CSCee84732

  Symptoms: The CPU utilization of a router that is configured for Multiprotocol Label Switching (MPLS) may temporarily increase to 80 or 90 percent when a peer router is reloaded or when an interface with a large number of numbered subinterfaces is administratively enabled.

  Conditions: The symptom is observed in a rare situation when label distribution protocol (LDP) is used in configurations with a very large number of numbered interfaces. When this problem occurs, the output of the **show process cpu sorted** command shows that the "Tagcon Addr" process consumes the majority of the CPU cycles.

  Workaround: There is no workaround.

- CSCef04163

  Symptoms: The subinterface of a link bundle member is not deleted when you reload microcode onto (or perform an OIR of) the line card on which the channel group is configured.

Conditions: This symptom is observed on a Cisco 12000 series when a large number of subinterfaces are configured on a port channel, when you remove a member from the channel group, and when you immediately afterwards reload microcode onto the line card. After the line card has come up, you cannot add members to the channel group until all the subinterfaces of the removed member are deleted. This situation occurs because of a race condition.

Workaround: Wait for a few seconds after you remove a member from the channel group before you reload microcode onto the line card.

- CSCef06050

  Symptoms: IPv6 unicast and multicast traffic may not recover on an Engine 4 plus (E4+) 1x10 GE line card after you have performed two software OIRs of the primary CSC.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0S.

  Workaround: Reload the E4+ 1x10 GE line card.

- CSCef06121

  Symptoms: An Engine 2 3-port Gigabit Ethernet line card may stop transmitting packets.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(24)S6.

  Workaround: Enter the **hw-module reload** command to enable the line card to resume transmitting packets.

- CSCef06858

  Symptoms: Line cards in a Cisco 12000 series may fail when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured with two PRPs and that runs a Cisco IOS interim release for Release 12.0(30)S when you enter the **redundancy force-switchover** command. Note, however, that this caveat is resolved in Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCef16379

  Symptoms: An Engine 2 8-port ATM line card may not forward traffic from a VRF.

  Conditions: This symptom is observed on a Cisco 12000 series when the prefix of the VRF is imported using an MPBGP tag.

  Workaround: There is no workaround.

- CSCef18515

  Symptoms: After you have entered the **clear cef line** command, when you enter the **show ip cef** command for the RP and for a line card, the output is inconsistent.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured for Fast ReRoute.

  Workaround: There is no workaround.

- CSCef22069

  Symptoms: On a Cisco 12000 series that functions as an egress PE router in an MPLS VPN network, after the customer-facing Gigabit Ethernet line card is reloaded, the ingress line card that receives an incoming VPN label with a destination with a glean adjacency (which requires an ARP) without a BGP session may not properly complete the adjacency, causing traffic to be dropped.

  Conditions: This symptom is mostly observed with static recursive route configurations. To recover from the symptom, manually ping the interface of the CE router from the adjacent PE router.

Workaround: Configure the static ARP entries for the nexthop router that is configured in the static recursive routes.

- CSCef25917

  Symptoms: A 4GE-SFP-LC line card may reload unexpectedly when it processes QoS traffic in a configuration with a VLAN on a VCG that is configured with an ingress CoS.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release when the resolved ARPs are deleted, for example, when routers flap, when BGP peers do not respond, or when you enter the **clear arp** command. Note that the symptom may also occur on releases earlier than Release 12.0(26)S.

  The ingress CoS includes a **set** command for the matched class: either a **police** command with a **set** command or a simple **set** command and either a **set-mpls** command or a **set-dscp** command.

  Possible Workaround: Configure static ARPs.

- CSCef26053

  Symptoms: Load-balancing does not work over a BGP multipath. Some of the traffic may be forwarded correctly while other traffic may be forwarded unlabeled into the MPLS core.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the following conditions are present:

  – The affected route is in a VRF.
  – One of the paths is learned from a CE router via an eBGP multihop session.
  – The eBGP multihop peer (that is, the CE router) is reachable through the MPLS core and the BGP session does not involve a label exchange.

  Workaround: Avoid a multihop eBGP session in which the CE router is reachable through the MPLS core. For example, instead of a configuration in which the CE router connects to the PE router across the MPLS core, configure the CE peer to connect to a local PE router that redistributes the routes it has learned from the CE peer to other PE routers. (The local PE router may need to be configured for eiBGP multipath.)

- CSCef26543

  Symptoms: A Cisco 12000 series line card may rate-limit process-switched packets to the GRP. This situation causes a ping to be lost when you perform a ping test to the local interface of the router.

  Conditions: This symptom is observed when the interface is configured for HDLC, when the interface has a hard loop, and when the IP address of the interface is the destination of the ping. Because the interface is in the up/up state (looped) and functional, there should be no packet loss when you ping the interface at its own IP address.

  Workaround: There is no workaround.

- CSCef29467

  Symptoms: When you enter commands in various configuration modes such as address-family, PVC, service-policy, and so on, an invalid input error message may be returned even though the command was accepted and entered into the running configuration. The following is an example:

```
Router(config-router-af)#redistribute connected
address-family ipv4 vrf atmTrk
  ^
```

  Invalid input detected at "^" marker.

Conditions: This symptom is observed on a Cisco 12410 that is configured with two Performance Route Processors (PRP-1) that function in Route Processor Redundancy (RPR) mode and that runs one of the following images:

- The c12kprp-p-mz image of Cisco IOS Release 12.0(24)S3.
- The c12kprp-p-mz image of Cisco IOS Release 12.0(23)S4.
- The c12kprp-k3p-mz image of Cisco IOS Release 12.0(27)S2

This list is not all-inclusive: the symptom may also occur in Release 12.0(20)S, Release 12.0(20)ST, and later releases.

The symptom occurs when the **do** command is interleaved between configuration commands.

Workaround: Verify that the configuration command is properly accepted by entering the **show running-config** command.

- CSCef33670

  Symptoms: An Engine 4 egress line card that switches traffic may reset when the ingress line card is shut down.

  Conditions: This symptom is observed on a Cisco 12000 series when the ingress line card is an Engine 3 POS line card and when IP-to-tag traffic is switched.

  Workaround: There is no workaround.

- CSCef39284

  Symptoms: A router may crash when you enter the **crypto key generate dss** *key-name* command.

  Conditions: This symptom is observed on a Cisco 12012 that is configured for SSH but may occur on any Cisco platform that is configured for SSH.

  Workaround: There is no workaround.

- CSCef40001

  Symptoms: When the **police cir percent** command is configured as a service-policy input on an MFR or MLP bundle CFI, the maximum bandwidth that is allocated by the service policy is a T1 link bandwidth.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S or an interim release for Release 12.0(30)S when a police-policy input is applied on the bundle CFI over a 1-port OC-12 channelized ISE line card. Note, however, that this caveat is resolved in Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCef44242

  Symptoms: Policing parameters may not be applied correctly, causing traffic to be dropper.

  Conditions: This symptom is observed when you apply ingress policies to a multilink interface.

  To verify if the parameters are applied correctly, enter the **show policy-map interface** *interface-name*. The CIR (in bps) shows whether or not the parameter was applied.

  Workaround: Remove the service policy and reapply it to the multilink interface.

- CSCef45609

  Symptoms: An Engine 3 Quad OC-12 line card that is configured with multicast VPNs may punt traffic to the RP when multicast is disabled by entering the **no ip multicast-routing distributed** command and then re-enabled by entering the **ip multicast-routing distributed** command.

Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(26)S4 or a later release but may also occur in other releases.

Workaround: There is no workaround.

- CSCef49138

  Symptoms: When you enter the **show policy-map interface** *interface-number* command, a router may crash because of a bus error exception.

  Conditions: This symptom is observed on a Cisco 12000 series when the **service-policy output** *policy-map-name* command is enabled on the same interface for which you enter the **show policy-map interface** *interface-number* command.

  Workaround: There is no workaround.

- CSCef53169

  Symptoms: An outbound ACL with a log/log-input keyword changes the IP destination address in the packets. As the result, packets that should be permitted are incorrectly denied.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(29)S when the incoming interface for the packets is a tag-switching interface. The symptom is observed irrespective of whether the interface with this outbound ACL is a tag-switching interface or not.

  Workaround: Do not use the log/log-input keyword in the ACL.

- CSCef53475

  Symptoms: Packet drops occur when traffic is sent below the shape rate that is defined in a service policy.

  Conditions: This symptom is observed on a Frame Relay interface when there are multiple DLCIs that have service policies enabled. Each DLCI has a hierarchical policy with a shape rate in the class default at the parent level and a child policy with LLQ and CBWFQ classes. When traffic to each DLCI is just below the shape rate and the combined traffic through the interface is close to line rate, packet drops occur on some DLCIs. The symptom does not occur when traffic is sent to one DLCI at the time.

  Workaround: Increase the shape rate to compensate for the scheduling inaccuracy.

- CSCef53570

  Symptoms: When IPv4 multicast is configured on an interface and when hardware forwarding is enabled, the interface stops forwarding all unicast and multicast traffic.

  Conditions: This symptom is observed only on Cisco 12000 series Engine 2 line cards.

  Workaround: Disable hardware forwarding.

- CSCef54021

  Symptoms: After an SSO switchover has occurred, traffic stops on interfaces that have both an input and an output policy attached.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: Remove and re-attach the policies to the interfaces.

- CSCef54679

  Symptoms: Time-based policing and shaping do not function on a 4-port OC-3 ATM ISE line card.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S when an input service policy is attached to a VC.

  Workaround: There is no workaround.

- CSCef54779

  Symptoms: Under a rare condition, when a main interface switches over to a backup interface on 4-port GE line card, a ping to another neighboring interface that is not at all related to the backup interface fails. A sniffer trace shows that the Src/Dst MAC address in the ICMP reply is that of the backup interface.

  Conditions: This symptom is observed on a Cisco 12000 series when you repeatedly disable the main interface that is associated with a backup interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCef55373

  Symptoms: The BGP process can take up 100 percent of the CPU for an extended period of time when 6PE is configured.

  Conditions: This symptom is observed on a Cisco 12000 series when a large number of IPv6 routes and 6PE labels are allocated.

  Workaround: There is no workaround.

- CSCef56327

  Symptoms: You may not be able to configure the **clock source line** command during the configuration of the SONET controller on a Cisco 7200 series in which a PA-MC-STM1 port adapter is installed.

  When you enter the **clock source line** command during the configuration of the SONET controller, the output of the **show running-config** command indicates that the clock source is set to line. However, the output of the **show controllers sonet** command indicates that the clock is set to internal, and when you enter the **show running-config** command again, the output indicates this time that the clock source is set to internal.

  Conditions: This symptom is observed when the PA-MC-STM1 port adapter is connected back-to-back via dark fiber to another PA-MC-STM1 port adapter.

  Workaround: Enter the **overhead s1byte ignore** command on the SONET controller before you configure the clock source.

- CSCef59140

  Symptoms: The protocol may go down on random link bundles that are part of the multilink Frame Relay (MFR) protocol on a Cisco 12000 series that is configured with a channelized OC-12 DS1 line card.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S after you have reloaded the router.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected link bundles.

- CSCef62246

  Symptoms: An Auto-RP mapping entry may expire when hardware acceleration is enabled on the VRF interfaces or when a static VRF RP statement is configured on the PE router.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router.

  Workaround: Disable hardware acceleration or define a static VRF RP statement with an ACL.

- CSCef64744

  Symptoms: On a 6-port channelized T3 line card that is enabled for QoS, a low latency queue (LLQ) may not receive traffic that is mapped to the LLQ.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1.

Workaround: Reload the line card. If this is not an option, there is no workaround.

- CSCef66562

  Symptoms: The cbQosPolicyMapName object may stop functioning.

  Conditions: This symptom is observed when an active view includes the ciscoPingMib.

  Workaround: Either remove the cisciPingMib or include the **lsystem** keyword in the same view by entering the **snmp-server view PingMIB lsystem included** command.

- CSCef67078

  Symptoms: A PXF buffer leak occurs on an L2TPv3 decapsulation router, which van be observed in the output of the **show hardware pxf cpu buffer** command:

```
router#show hardware pxf cpu buffer
FP buffers
pool   size    # buffer    available   allocate failures    low buffer drops
------------------------------------------------------------------------------
0      9344    1293        1293        0                    0
1      1664    12930       12930       0                    0
2      640     26746       127         0                    77165
3      256     34072       34072       0                    0
4      128     59934       59934       0                    0
```

  Depending on the packet size, the buffer leak can occur in different pools.

  Conditions: The symptom is observed on a Cisco 10720 in the following two scenarios:

  - An MPLS-enabled interface is the network backbone for L2TPv3 tunnels.
  - An 802.1q interface is the network backbone for L2TPv3 tunnels and an input security ACL with more than 400 lines is configured on the 802.1q backbone interface.

  Workaround: There is no workaround.

- CSCef67267

  Symptoms: The Fast ReRoute database shows all prefixes in the active state.

  Conditions: This symptom is observed on a Cisco router after a connected point of local repair (PLR) has rebooted.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the primary tunnel is configured. Doing so restores the prefixes to the ready state.

- CSCef67840

  Symptoms: When the CEF table consistency checker is configured to perform a passive scan check of tables of the line cards, the CEF table consistency checker may report false inconsistencies, which you can view in the output of the **show ip cef** *ip-address* command. The false inconsistencies may occur because of a race condition.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

  If an inconsistency is reported for a recursive loadbalanced route for which the output interfaces for the next-hop IP address differ between the RP and line card, you can ignore this inconsistency because this information is not used during the forwarding process.

Workaround: Disable the CEF table consistency checker so that no passive scan check is performed of tables of the line cards.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

- CSCef69146

  Symptoms: A Cisco 12000 series crashes when the encapsulation of T1 channels is changed to MFR during a cut-and-paste operation of the configuration or when you copy from a file to the running configuration.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that is configured with a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card when the configuration is changed at a fast pace. When the configuration lines are entered at a slower pace, the symptom does not occur.

  Workaround: Avoid pasting configuration files to the 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card. If this is not an option, there is no workaround.

- CSCef72305

  Symptoms: A standby PRE crashes on bootup.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 1000 ATM VCs when a forced SSO switchover occurs.

  Workaround: There is no workaround.

- CSCef72411

  Symptoms: Line cards and the standby RP on a Cisco 12000 series may fail when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that has two PRPs when you enter the **redundancy force-switchover** command. Note that this caveat is resolved in Release 12.0(30)S.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the RP to recover from a Fabric Interface ASIC (FIA) halt condition if this condition occurs following an RP switchover. In a Cisco IOS software release that does not integrate the fix for this caveat, the RP does not attempt to recover from a FIA halt condition after an RP switchover has occurred (but it does attempt to recover from such a conditions in other situations).

- CSCef72555

  Symptoms: When you change the Cisco IOS software image on a Cisco 10000 series, HA may function differently, causing strange behavior, a standby crash, or both.

  Conditions: This symptom is observed when you change the Cisco IOS software image on a Cisco 10000 series from one release train to another release train. This symptom affects Release 12.0S, Release 12.2S, releases that have been derived from Release 12.2 releases, and releases that have been derived from Release 12.3.

Workaround: There is no workaround.

- CSCef78098

  Symptoms: An Engine 1 or Engine 2 Gigabit Ethernet (GE) line card may stop switching traffic even though the line protocol is up. Pings and routing do not work, and traffic does not go through.

  Conditions: This symptom is observed a Cisco 12000 series after error recovery and when the **negotiation auto** command is not configured for the interface of the GE line card.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface of the line card.

- CSCef80260

  Symptoms: IP packets with an IP length that is smaller than 64 bytes and that have the More Fragments (MF) flag set to 1 do not go through a Cisco 12000 series.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3 or Release 12.0(28)S1 and that is configured with a 2-port OC-48 DPT Engine 4+ ingress line card.

  Workaround: There is no workaround.

- CSCef80349

  Symptoms: An MPLS traffic engineering (TE) tunnel may not come back up after a link flaps.

  Conditions: This symptom is observed when the headend of the TE tunnel is a third-party router that has the **no cspf** command configured for the label switched path (LSP) and when the tunnel midpoint is a Cisco router that runs Cisco IOS Release 12.0(25)S1. The symptom occurs when the link downstream (that is, towards the tailend of the tunnel) on the Cisco router fails because the interface on either side of the link is shut down.

  In addition, note that the third-party router does not increment the LSP ID when it receives a message, nor does it send a PathTear message in response to a PathErr message.

  Possible Workaround: Use an explicit path on the third-party router but without the **no cspf** command enabled.

- CSCef81555

  Symptoms: The running configuration does not show the correct policing rate if the rate is configured to be larger than 4,200,000,000 bps.

  Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCef82700

  Symptoms: A 4-port Gigabit Ethernet (GE) line card generates TCAM errors when a large QoS configuration is applied. The following messages are generated:

  ```
  %QM-2-TCAM_ERROR: TCAM pgm error(8): ACL Merge Failed
  %QM-4-SW_SWITCH: Interface GigabitEthernet2/0 routed traffic will be software
  switched in egress direction(s)
  ```

  In addition, when you modify the policy map while it is still attached to the interface of the 4-port GE line card, the TCAM utilization goes up drastically; however, when you remove the policy map from the interface, the TCAM utilization is not brought back to zero.

  Conditions: These symptoms are observed on a Cisco 12000 series when a child policy map with 75 or more customers is applied and when each child policy has at least 6 queues.

Workaround: Change the default merge algorithm to POD by entering the **hw-module slot** *slot-number* **reload** command for the slot in which the affected line card is installed.

Alternate Workaround: To avoid problems with the policy map modification, remove the service policy from the interface, modify the service policy, and reattach the service policy to the interface.

- CSCef83864

  Symptoms: A Cisco 10000 series reloads unexpectedly.

  Conditions: This symptom is observed when 750 VRFs are configured.

  Workaround: There is no workaround.

- CSCef86176

  Symptoms: The following CLI commands are missing from a Cisco 12000 series:

```
router(config)#map-class frame-relay r
router(config-map-class)#frame-relay ?
  adaptive-shaping   Adaptive traffic rate adjustment, Default = none
  bc                 Committed burst size (Bc), Default = CIR
  be                 Excess burst size (Be), Default = 0 bits
  cir                Committed Information Rate (CIR), Default = 56000 bps
  custom-queue-list  VC custom queueing
  fecn-adapt         Enable Traffic Shaping reflection of FECN as BECN
  mincir             Minimum acceptable CIR, Default = 1/2 CIR
  priority-group     VC priority queueing
  traffic-rate       VC traffic rate
```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

- CSCef89562

  Symptoms: An Engine 4+ EPA-GE/FE-BBRD line card reports "%TX192-3-PAM_MODULE" and "%TX192-3-PAM_PIM" errors, and the interfaces continue to flap with the following error message:

```
%GRPGE-6-INVALID_WORD: Interface GigabitEthernet15/1/0: Detected RX Invalid Word
```

  When there is heavy traffic, the line card may crash without generating any crashinfo.

  Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 or Release 12.0(27)S3.

  Workaround: There is no workaround.

- CSCef91030

  Symptoms: After the default route is received from a remote PE for a VRF, communication stops for traffic via the default route in this VRF on a Cisco 12000 series that functions as a PE router in an MPLS VPN environment. The packets are switched out of the core MPLS interface untagged as native IPv4 packets instead of with MPLS and BGP labels.

  Conditions: This symptom is observed when the traffic is received from VRF interfaces on an Engine 2 line card that is installed in a Cisco 12000 series that functions as a PE router.

  The symptom occurs in Release 12.0(27)S2, Release 12.0(27)S3, and interim releases for Cisco IOS Release 12.0(30)S. Other releases may be affected too. The symptom does not occur in Release 12.0(24)S2.

The symptom occurs when the VRF ingress interface is configured on an Engine 2 3-port GE line card or Engine 2 1-port OC-48 POS line card. Other line cards may be affected too. The symptom does not occur when the VRF ingress interface is configured on an Engine 0 4-port OC-3 POS line card or 4-port GE ISE line card.

Workaround: There is no workaround.

- CSCef91170

  Symptoms: A Cisco 12000 series that has a CHOC12/DS1 ISE line card that is configured for mVPN over multilink PPP may not maintain PIM neighbors over GRE tunnels.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S2, 12.0(27)S3, or 12.0(28)S1.

  Workaround: On the multilink interface, enter the following sequence of commands:

```
Router(config)# interface multi1
Router(config-if)# no ip pim sparse-dense-mode
Router(config-if)# ip pim sparse-dense-mode
```

  Doing so enables the PIM neighbor to come up across the GRE tunnel.

- CSCef91475

  Symptoms: A CPUHOG situation may occur intermittently on a Cisco 12000 series, causing fabric pings to be lost and all OSPF and BGP adjacencies to be dropped.

  Conditions: This symptom is observed in PRP on a Cisco 12000 series router.

  Workaround: There is no workaround. However, the symptom resolves itself.

- CSCef92153

  Symptoms: When a VRF VLAN subinterface punts a packet such as an ARP or ICMP packet to the CPU of the line card, the main interface is unable to process a packet such as ICMP packet that is destined for the main interface. When BGP packets enter and leave via the main interface, a BGP neighbor may go down.

  These symptoms do not affect non-VRF subinterfaces, only the main interface. Transit packets that pass through the main interface are not affected.

  When a non-VRF VLAN subinterface punts a packet to the CPU of the line card, the main interface may return to normal operational.

  Conditions: These symptoms are observed on an Engine 4+ Gigabit Ethernet line card that is installed in a Cisco 12000 series that runs Cisco IOS Release 12.0 (25)S. Engine 2 and Engine 3 line cards are not affected. For the symptoms to occur, all of the following conditions must be present:

  – A VRF VLAN subinterface is configured on the Engine 4+ line card.
  – The main interface is also used with an IP address assigned to it.
  – The VRF VLAN subinterface receives a packet such as an ARP or ICMP packet that is punted to the CPU of the line card.

  For the BGP neighbor to go down, in addition to the above-mentioned conditions, the **neighbor** *ip-address* **password** *string* command must be configured.

  Workaround: If you must use a VRF VLAN subinterface, create another subinterface for non-VRF communication on the same main interface.

  Alternate Workaround: Do not use a VRF VLAN subinterface.

- CSCef93354

  Symptoms: When MLP and SSO are configured and interfaces in a multilink bundle flap, the secondary PRE does not handle this situation correctly. When a PRE switchover occurs, the MLP bundle may enter an inappropriate state.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround. To recover from the symptom, reload the Cisco 10000 series.

- CSCef94619

  Symptoms: A VIP may crash while forwarding packets or a watchdog timeout crash may occur on the VIP during statistics collection.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 and that runs Cisco IOS Release 12.0(26)S4.

  Workaround: There is no workaround.

- CSCef96652

  Symptoms: The offered rate counter in the output of the **show policy-map interface** command is inaccurate.

  Conditions: This symptom is observed on a Cisco 12000 series when very high traffic rates are used.

  Workaround: There is no workaround.

- CSCef97536

  Symptoms: When Multiprotocol Label Switching (MPLS) label distribution protocol (LDP) is configured and you enter the **clear ip route** EXEC command, the MPLS forwarding entries for some of the cleared routing prefixes may become unlabeled.

  Conditions: This symptom is observed for prefixes that are connected (with an unspecified nexthop IP address) and that are not locally recognized. This situation may occur in a configuration in which two LDP peers are connected by a point-to-point link that uses PPP encapsulation, and in which both interfaces are configured to use IP addresses with /32 masks.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee12379. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Possible Workaround: Prevent the symptom from occurring by using a shorter network mask when you configure the interfaces or by using another encapsulation such as HDLC.

  When the symptom occurs, restore proper operation by forcing the LDP session that is associated with the link to re-establish itself, or by forcing the LDP session to re-advertise labels for the affected prefixes. The LDP session can be reset by entering the **clear mpls ldp neighbor** command, by administratively disabling and then re-enabling one of the interfaces, or by deconfiguring and then reconfiguring LDP on one of the interfaces. The LDP session can be forced to re-advertise labels by modifying the outbound label filtering configuration. However, this method is complicated and should only be attempted if you are already very familiar with the required procedures, and if the routers do not already have a complicated label filtering configuration in place.

- CSCef97964

  Symptoms: A VIP4-80 crashes when you enter the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(28)S1 and that is configured for SSO.

  Workaround: There is no workaround.

- CSCeg00111

  Symptoms: Padded IP fragments with an IP length that is shorter than 64 bytes and the More Fragments (MF) (which is set to 1) are dropped by an Engine 4+ line card that functions as an egress line card.

  Conditions: This symptom is observed when the ingress line card is an Engine 4+ DPT line card and the egress line card is any Engine 4+ line card.

  Workaround: There is no workaround.

- CSCeg00252

  Symptoms: When you enter the **show sec-disk0:** command or the **execute-on slot** *slot-number command* command on the standby RP, no command output is generated.

  Conditions: This symptom is observed on a Cisco 12000 series that has dual RPs and that is configured for RPR, RPR+, or SSO redundancy mode. Note that when you enter the **dir sec-disk0:** command on the standby RP, command output is properly generated.

  Workaround: There is no workaround.

- CSCeg00338

  Symptoms: A high CPU utilization may occur at the interrupt level on a Cisco 10000 series when CLNS traffic is forwarded.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with an PRE-1 and that runs Cisco IOS Release 12.0(24)S6.

  Workaround: There is no workaround.

- CSCeg01168

  Symptoms: Counters that are displayed in the output of the **show interface** commands for an ATM interface of an 8-port OC3 ATM line card show incorrect input packet and byte counts.

  Conditions: This symptom is observed on a Cisco 12000 series when the Port Mode Cell Relay Support feature is configured on the ATM interface.

  Workaround: There is no workaround.

- CSCeg01543

  Symptoms: A Cisco 7500 series VIP may crash when its serial interfaces are part of a Multipoint Frame Relay (MFR) bundle.

  Conditions: This symptom is observed when a Frame Relay end-to-end fragment is received on an MFR interface.

  Workaround: Administratively shut down the MFR interface or shut down the MFR interface on the other side of the link.

- CSCeg02511

  Symptoms: A Cisco 10000 series may display %CHSTM1-3-STATESYNC error messages, and a buffer leak may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S2 when a Fast Ethernet interface is configured to use DHCP via the **ip address negotiated** command.

  Workaround: Do not configure the **ip address negotiated** command. Rather, configure a specific IP address.

- CSCeg03055

  Symptoms: Sampled NetFlow may stop functioning.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S3 or a later release and that is configured with an Engine 4 plus 4-port OC-48 line card when the hardware of the line card is reset as a result of an error recovery process.

Workaround: Disable and re-enable Sampled NetFlow.

- CSCeg03180

  Symptoms: A line card in slot 15 is stuck in the WAITRTRY state.

  Conditions: This symptom is observed on a Cisco 12816 that is configured with dual RPs when an RP switchover followed by a CSC switchover occurs.

  Workaround: Reload the router.

  Alternate Workaround: Power down and power up the router.

- CSCeg06618

  Symptoms: A 6-port channelized T3 line card and a 2-port Channelized OC-3 line card may continuously generate the following error message:

  ```
  %LC_CX3-2-PLIM_CPU_CRASHED: PLIM CPU Tofab755 - plim reset
  ```

  Controllers and interfaces do not recover.

  Conditions: This symptom is observed on a Cisco 12000 series and occurs because of a problem with the recovery mechanism following a forced reset of the PLIM component of the line card. The symptom is visible only if another problem indirectly triggers a forced reset of the PLIM component.

  Workaround: There is no workaround. To recover the affected line card, reload the line card by entering **hw-module slot** *slot-number* **reload** command.

- CSCeg10276

  Symptoms: A routing loop occurs when you enter the **mpls traf-eng tunnel reoptimize** command on a PRP.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that is configured with an Engine 3 line card through which traffic enters and leaves.

  Workaround: Enter the **clear cef linecard** command on the interfaces that are affected by the routing loop.

- CSCeg10310

  Symptoms: A DSX3 interface of an ESR-8E3/DS3 line card is stuck in the initializing/down state.

  Conditions: This symptom is observed on a Cisco 10008 after the router is reloaded with Cisco IOS Release 12.0(28)S1.

  Workaround: Enter the **shutdown** controller configuration command followed by the **no shutdown** controller configuration command on the DSX3 controller of the affected interface.

- CSCeg10642

  Symptoms: When six queues are configured on an interface and some of the queues do not have traffic, the bandwidth of those inactive queues should be given to other active queues (queues with traffic) in proportion to their EIR (configured via bandwidth remaining). However, this is not the case. The bandwidth is not proportionally given to all the queues.

  Conditions: This symptom occurs when configuring a policy map that creates six queues in an interface.

  Workaround: There is no workaround.

- CSCeg11421

  Symptoms: A Cisco 10720 crashes when you delete an IPv6 ACL.

  Conditions: This symptom is observed when you delete the IPv6 ACL during the TurboACL compilation.

  Workaround: Wait for the ACL to be fully compiled before you delete it.

- CSCeg13868

  Symptoms: When the **no tag-switching ip propagate-ttl** command is configured on PE routers and a traceroute is executed from one CE router to a remote CE router, an egress PE router replies to the traceroute with the address of its ingress MPLS interface.

  Conditions: This symptom is observed only when the traceroute is destined for a network between an egress PE router and a remote CE router, when the ingress line card of the egress PE router is a Cisco 12000 series Engine 0 or Engine 1 line card.

  Workaround: There is no workaround.

- CSCeg15191

  Symptoms: An OC192E/POS-IR-SC line card resets with the following error messages:

  ```
  %MBUS_SYS-3-NOBUFFER: Message from slot 3 in stream 1 dropped
  %MDS-2-LC_FAILED_IPC_ACK: RP failed in getting Ack for IPC message of size 232 to LC
  in slot 3 with sequence 47350, error = timeout %FIB-3-FIBDISABLE: Fatal error, slot
  3: IPC Failure: timeout
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1.

  Workaround: There is no workaround.

- CSCeg16631

  Symptoms: When you enter the **distribute-list** *interface* command in a global RIP routing context and the interface that is specified in the command is a VRF interface, the command is rejected with the following error message:

  % The interface is not in the same VRF as the process

  Because the **distribute-list** *interface* command is not implemented in the IPv4 VRF address-family, there is no other way to filter networks received in updates via a VRF interface.

  Conditions: This symptom is observed in all Cisco IOS releases that integrate the fix for CSCee32557. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee32557. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: In a configuration that is mentioned above, to filter networks received in updates, enter the **distribute-list** *extended-ACL-reference* command in which the "source-part" of the extended ACL specifies the prefixes and the "destination part" matches on the IP address of the RIP neighbor.

- CSCeg28402

  Symptoms: Spurious memory accesses may occur on a Cisco 7500 series and may cause high CPU usage on the RSP.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed Multilink PPP (dMLP) and that functions in an MPLS network.

  Note that packet switching for MPLS packets over MLP bundles is not supported at the RSP level in Cisco IOS Release 12.0S.

Workaround: There is no workaround.

Further Problem Description: The fix for this caveat causes packets that are sent to the RSP for switching to be dropped. Distributed forwarded packets are forwarded correctly.

- CSCeg30179

  Symptoms: Removing a policy that has shape and bandwidth in the same class (in that same order) may cause a router to crash.

  Conditions: This symptom is observed when the router functions under a traffic load.

  Workaround: There is no workaround.

- CSCeg31912

  Symptoms: Ingress policing and bandwidth percent per-class do not function and limit traffic at the configured bandwidth for MLFR links. The output of the **show policy-map interface** command shows the configured bandwidth which differs from the actual bandwidth.

  Conditions: This symptom is observed on a Cisco 7500 series after the router is reloaded.

  Workaround: Remove the service policy and re-apply it to interface to enable correct calculation of the interface bandwidth.

- CSCeg33229

  Symptoms: A VIP may crash when an ingress service policy is removed from an MFR interface.

  Conditions: This symptom is observed on a Cisco 7500 series while traffic is being processed on the MFR interface.

  WorkAround: There is no workaround.

- CSCin74180

  Symptoms: Spurious memory accesses may occur on a VIP in which one or more channelized port adapters are installed. The CPU utilization may increase to 99 or 100 percent, causing the performance of the VIP to be impacted.

  Conditions: These symptoms are observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(6) but may also occur in other releases.

  Workaround: There is no workaround.

- CSCin75482

  Symptoms: A router may hang or crash when PA-MC-8TE1+ or PA-MC-2T3+ interfaces are congested with traffic and a QoS configuration such as shaping is configured on the interfaces.

  Conditions: This symptom is observed on a Cisco 7200 series but may also occur on other platforms.

  Workaround: Avoid congesting the interfaces.

- CSCin78324

  Symptoms: A Cisco 7200 VXR router may hang.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that has a PA-MC-8TE1 and that is configured for IPSec encryption, either via tunnel protection or via a crypto map.

  Workaround: Disable IPSec encryption.

- CSCin78325

  Symptoms: A serial interface of a PA-MC-8TE1+ continues to process packets even after the interface is placed in the "ADMINDOWN" state. The counters in the output of the **show interfaces serial** command may continue to increment even if the serial interface is shut down.

Conditions: This symptom is observed on a serial interface of a PA-MC-8TE1+ when there is a channel-group configuration for the interface.

Workaround: Remove the channel-group configuration for the interface.

- CSCin79436

  Symptoms: A Cisco 12000 series does not fragment IP traffic while switching the traffic into the MPLS core even when the size of the incoming IP packets exceeds the IP MTU of the egress interface. This situation causes the traffic to be dropped on the next hop router.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(26)S or a later release when all of the following conditions are present:

  – The traffic leaves through an egress interface of an Engine-3 line card (on the MPLS core side).
  – The imposed label stack contains only explicit null labels.
  – The size of the incoming IP packets exceeds the IP MTU of the egress interface.

  Workaround: Ensure that the IP MTU of the egress interface exceeds the maximum size of the incoming IP packets.

- CSCin79899

  Symptoms: When error recovery is performed on a 3-port Gigabit Ethernet (GE) line card that has port 0 in the shutdown state, the 3-port GE line card stop passing traffic on all ports.

  Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(23)S or a later release and that is configured with an Engine 2 3-port line card.

  Workaround: Reload the 3-port GE line card and leave port 0 in the up/down state.

- CSCin82862

  Symptoms: Multicast traffic is not switched from a multilink interface on a Cisco 7500 series that is configured for distributed multilink PPP (MLP).

  Conditions: This symptom is observed when the router is reloaded or when the multilink interface flaps.

  Workaround: Enter the **clear ip mds linecard *** command on the Route/Switch Processor (RSP).

- CSCin83445

  Symptoms: Incoming multicast traffic on a distributed MLP link is process-switched.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed MLP after the router has been reloaded.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink interface.

- CSCsa46154

  Symptoms: A Route Processor (RP) failover occurred.

  Conditions: This symptom occurred while using the **show route-map** command in one session and removing several route-maps in rapid succession in another session.

  Workaround: Do not use the **show route-map** command while removing route-maps in a concurrent vty session.

- CSCuk52952

  Symptoms: An Engine 3 ATM line card may continuously crash.

Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S after you configure IP QoS on an ATM interface of the line card. Note, however, that this caveat is resolved in Release 12.0(30)S.

Workaround: There is no workaround.

Wide-Area Networking

- CSCef45502

  Symptoms: A connection remains to exist on a line card even though the connection is deleted on the RP.

  Conditions: This symptom is observed on a Cisco 12000 series when you enter the **no frame-relay interface-dlci** command.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCef77523

  Symptoms: The protocol may go down on random Multilink Frame Relay (MFR) link bundles.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S and that is configured with a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card after you have reloaded the router. The symptom may also occur in other releases such as Release 12.2S and Release 12.3.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCef82683

  Symptoms: An MFR bundle may stay in the down state after redistributing bundle links. The output of the **show frame-relay multilink** command displays as cause code “inconsistent bundle.”

  Conditions: This symptom is observed when a Remove-Link message is lost.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected bundle.

- CSCin05330

  Symptoms: When a multilink bundle interface is created by entering the **interface multilink** *group-name* global configuration command, the Cisco Discovery Protocol (CDP) becomes incorrectly disabled. If the **cdp enable** interface configuration command is used to enable CDP on the multilink bundle interface, the command is not saved in the startup configuration and CDP remains disabled after the router is reloaded.

  Conditions: This symptom is observed on a Cisco platform that is configured with a multilink bundle interface.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(28)S1

Cisco IOS Release 12.0(28)S1 is a rebuild of Cisco IOS Release 12.0(28)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(28)S1 but may be open in previous Cisco IOS releases. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdx55178

  Symptoms: Difficulties may occur when you attempt to remotely log in to a Cisco router that supports ATM. After you have established a virtual terminal connection to the system, the following user access verification sequence may be displayed, and the connection terminated:

  ```
  Password:
  Password:
  Password:
  % Bad passwords
  ```

  Conditions: This symptom is observed on a Cisco router that support ATM when an interactive ATM ping is terminated abnormally.

  Workaround: Instead of using an interactive ATM ping, enter the **ping atm interface** *atm interface vpi vci* [**seg-loopback** | **end-loopback**] [*repeat* [*timeout*]] privileged EXEC command.

- CSCea21328

  Symptoms: After a Versatile Interface Processor (VIP) has reloaded, there does not seem to be a crashinfo file because the crashinfo file is not closed; therefore, it is not visible or accessible. If the same VIP reloads again, both the first and second crashinfo files are accessible.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(6f). The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCec69536

  Symptoms: When you reload a Cisco 7500 series router with a new Cisco IOS software image, the router may reload unexpectedly during the bootup process and generate an “Imprecise cache parity error” message.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Route Switch Processor 8 (RSP8) and that runs Cisco IOS Release 12.0 S or Release 12.2(18)S when you reload the router with an image of Cisco IOS Release 12.3 T.

  Workaround: Do not reload the router. Rather, power-cycle the router to properly load the image of Cisco IOS Release 12.3 T.

- CSCed33110

  Symptoms: A VIP crash may cause memory exhaustion on an RSP, which in turn may cause the RSP to crash.

  Conditions: This symptom is observed more frequently on routers with a high IDB count.

  Workaround: There is no workaround.

- CSCed75238

  Symptoms: A serial interface on a Cisco 7500 series may stop transmitting traffic and may report the following VIP crashes:

```
%MDS-2-LC_FAILED_IPC_ACK: RP failed in getting Ack for IPC message of size 84 to LC
in slot 2 with sequence 1007, error = timeout %RSP-3-RESTART: interface Serial3/0/0:0,
not transmitting

%VIP2-3-MSG: slotX VIP-3-SVIP_CYBUSERROR_INTERRUPT: A Cybus Error occurred.
%VIP2-1-MSG: slotX CYASIC Error Interrupt register 0x4000000 %VIP2-1-MSG: slotX DMA
Transmit Error %VIP2-1-MSG: slotX CYASIC Other Interrupt register 0x100 %VIP2-1-MSG:
slotX QE HIGH Priority Interrupt %VIP2-1-MSG: slotX QE RX HIGH Priority Interrupt
%VIP2-1-MSG: slotX CYBUS Error Cmd/Addr 0xD00FF3A
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(5a) but may also occur in other releases. This symptom is not observed in Release 12.1(8c).

Workaround: There is no workaround.

- CSCed86286

  Symptoms: A router may reload due to a software-forced crash.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.2(13)T5 and that has SSH configured. However, the symptom may occur on other platforms that run other releases and that do not have SSH configured.

  Workaround: There is no workaround.

- CSCee35740

  Symptoms: After a VIP crashes, a FIB-3-FIBDISABLE error message due to an IPC timeout may occur for all the slots of the VIP.

  Conditions: This symptom is observed on a Cisco 7500 series after the VIP crashes and before the VIP recovers. The FIB-3-FIBDISABLE error message is generated for all the slots of the VIP, causing dCEF switching to become disabled.

  Workaround: There is no workaround. You can reenable dCEF by entering the **clear cef linecard** command.

- CSCee39972

  Symptoms: A Cisco router may experience a memory leak in the IPC buffers:

```
Interface buffer pools:
IPC buffers, 4096 bytes (total 41664, permanent 624):
     0 in free list (208 min, 2080 max allowed)
     3339198 hits, 75195 fallbacks, 0 trims, 41040 created
     4254 failures (65497 no memory)
```

  You can also see that the Pool Manager process is holding onto more and more memory:

```
PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   5   0  246913476   44522964  202605044  176561380    2654280 Pool Manager
```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or 12.0(26)S1. The memory leak is triggered by the SNMP polling of specific OIDs within the ciscoEnhancedMemPoolMIB MIB.

  Workaround: Prevent the MIB from being polled by explicitly configuring an SNMP view in the Cisco IOS configuration. To prevent this MIB from being accessed via any community strings, create a view and apply the view to all communities configured, such as:

```
snmp-server view NOMEMPOOL iso included
snmp-server view NOMEMPOOL ciscoEnhancedMemPoolMIB excluded
snmp-server community public1 view NOMEMPOOL ro 6
```

```
snmp-server community public2 view NOMEMPOOL ro 7
snmp-server community public3 view NOMEMPOOL ro 8
```

The specific MIB that is being blocked is the ciscoEnhancedMemPoolMIB MIB (1.3.6.1.4.1.9.9.221).

Once the configuration is in place, the router must be reloaded to clear the IPC cache and free the memory.

- CSCee60844

  Symptoms: A software-forced crash may occur on a Cisco 7500 series.

  Conditions: This symptom is observed on a Cisco 7500 series with a PA-T3 or PA-2T3 configured for class-based weighted fair queueing (CBWFQ).

  Workaround: Remove CBWFQ from the interface or policy map.

- CSCee63808

  Symptoms: A router reloads when you enter the **show monitor event-trace merged-list** *component* command and you use a long string for the *component* argument.

  Conditions: This symptom is observed on a Cisco 7200 and Cisco 7500 series that run Cisco IOS Release 12.2 S.

  Workarounds: Enter a short string for the *component* argument.

- CSCee78266

  Symptoms: A Cisco 7500 series may reload in an indefinite loop when you unintentionally enter the **show list** *number* hidden command.

  Conditions: This symptom is observed when you, for example, abbreviate the **show line 2000** command as the **show li 2000** command and actually execute the **show list 2000** hidden command.

  Workaround: Do not abbreviate the **show line** command as the **show li** command but enter the full command.

- CSCin44135

  Symptoms: A slave RSP running in HSA mode may crash with a cache parity exception.

  Conditions: This symptom is observed on a Cisco 7500 series and occurs only when the slave RSP is an RSP8 or RSP16 that runs in HSA mode.

  Workaround: There is no workaround.

  The fix for this caveat turns off the L3 cache by default on an RSP8 or RSP16 that functions as a slave and that runs in HSA mode; you do not need to do anything specific to turn off L3 cache by default on an RSP8 or RSP16 that functions as a slave and that runs in HSA mode.

  For an RSP8 or RSP16 that functions as a slave and that runs in a non-HSA mode such as RPR, you can turn off the L3 cache by entering the **l3 cache bypass** command on the master RSP while the slave RSP8 or RSP16 still runs in a non-HSA mode.

  Because the slave RSP performs non-CPU intensive operations, regardless of the mode of operation, turning off the L3 cache does not have any undesirable impact.

EXEC and Configuration Parser

- CSCee64504

  Symptoms: A CPUHOG may occur for about 4.5 seconds when you enter the **show running-config** command.

  Conditions: This symptom is observed on a Cisco uBR10000 series but may also occur on other platforms.

  Workaround: Do not enter the **show running-config** command. Rather, enter the **show config** command.

  Further Problem Description: The **show tech-support** command also has a problem when it reaches the **show running-config** command part. Changing the term length does not work as workaround.

Interfaces and Bridging

- CSCec15909

  Symptoms: In a High Availability (HA) environment with Stateful Switchover (SSO) enabled and while trying to configure framing for T1 on T3 PA, the standby route processor (RP) gets reloaded giving a “CCB playback failed” error.

  Conditions: The defect is seen with SSO or RPR-Plus enabled on T3 family of port adaptors. The trigger is the change in framing configuration for T1 on T3 PA.

  Workaround: Administratively shutdown all interfaces on T1 before changing the framing.

- CSCed75174

  Symptoms: A router may not forward VLAN traffic.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(28)S when there are no features configured under VLAN.

  Workaround: There is no workaround. The symptom does not occur in Release 12.0(25)S1.

- CSCee25605

  Symptoms: When you enter the **show ip interface brief**, the output indicates that a serial subinterface has a down status and that the protocol is down too:

```
router# show ip interface brief
Interface     IP-Address      OK? Method Status                Protocol
Ethernet0/0   10.7.0.68       YES NVRAM  up                    up
Ethernet0/1   unassigned      YES NVRAM  administratively down down
Ethernet0/2   unassigned      YES NVRAM  administratively down down
Ethernet0/3   unassigned      YES NVRAM  administratively down down
Ethernet0/4   unassigned      YES NVRAM  administratively down down
Ethernet0/5   unassigned      YES NVRAM  administratively down down
Serial4/0     unassigned      YES NVRAM  administratively down down
Serial4/1     unassigned      YES NVRAM  administratively down down
Serial4/2     unassigned      YES NVRAM  administratively down down
Serial4/3     unassigned      YES NVRAM  administratively down down
Serial4/4     unassigned      YES NVRAM  administratively down down
Serial4/5     unassigned      YES NVRAM  administratively down down
Serial4/6     unassigned      YES NVRAM  administratively down down
```

```
Serial4/7     unassigned      YES NVRAM  administratively down down
Serial5/0:23  10.0.0.1        YES NVRAM  down                   down
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 when you attempt to configure the interface and bring it up.

Workaround: There is no workaround.

- CSCee47714

  Symptoms: Entering the **shutdown** command on a controller of a Packet over T1/E1 Network Transceiver puts the controller permanently down. Entering the **no shutdown** command on the controller does not bring the controller up.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S and is specific to the controller that is installed in a PA-MC-8T1/E1, PA-MC-4T1/E1, or PA-MC-2T1/E1 port adapter.

  Workaround: There is no workaround.

- CSCee58873

  Symptoms: The **show controllers t1** *slot/port* command may show only the current interval.

  Conditions: This symptom is observed on a Cisco 7200 series when FDL is configured.

  Workaround: There is no workaround.

  Further Problem Description: When FDL is configured, the router updates the MIB data after checking for a valid local and remote MIB data interval that it receives from the T1 port adapter. During the remote MIB update, and if the received data interval is invalid, the router clears both the remote and the local data instead of clearing only the remote data and starting again.

- CSCin66616

  Symptoms: The output of an snmpwalk for the entPhysicalDescr MIB on a PA-MC-8E1/120 may shows the PA-MC-8E1/120 as unknown.

  Conditions: This symptom is observed on a Cisco 7500 series in which a PA-MC-8E1/120 in installed.

  Workaround: There is no workaround.

- CSCin67296

  Symptoms: Channelized interfaces on a channelized T3 line card or port adapter that is configured for Frame Relay encapsulation may be in the up/down state, and DLCIs are inactive.

  Conditions: This symptom is observed when you reload a Cisco platform and when the interfaces were in the up/up state before you reloaded the platform.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller of either the T3 line card or port adapter on the Cisco platform or on the T3 line card or port adapter on the platform at the remote end.

  Alternate Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the main interface on the Cisco platform.

- CSCin74070

  Symptoms: Performance degrades when the number of VCs through which traffic is sent is scaled for PCRoMPLS AToM VCs.

  Conditions: This symptom is seen on a Cisco 7500 series with a PCRoMPLS configuration on VCs.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCds67028

  Symptoms: A Cisco 7200 series router may reload with a bus error in ipigrp2_ager.

  Conditions: This symptom can occur while the router is running Enhanced Interior Gateway Routing Protocol (EIGRP).

  Workaround: There is no workaround.

- CSCed33044

  Symptoms: ARP may not function properly on the remote side of point-to-point Fast Ethernet link with a default static route until the remote side is pinged.

  Conditions: This symptom is observed on a Cisco router when ARP and /31 mask are configured on a point-to-point link Fast Ethernet link with a default static route. The symptom is platform-independent.

  Workaround: There are four different workarounds:

  - Use a /30 netmask on the point-to-point Fast Ethernet connection.
  - Configure a static ARP entry for the remote side of the Fast Ethernet link.
  - Enter the **ip proxy-arp** command on the remote side of the Fast Ethernet link.
  - Use an OSPF route instead of a default static route.

- CSCed57403

  Symptoms: When a Cisco router is a midpoint of a TE tunnel and the tunnel headend is a third- party vendor router, the Cisco router may crash.

  Conditions: This symptom is observed during a period of network instability and may occur when a TE tunnel does not contain an EXPLICIT ROUTE object and when the tunnel is dynamically routed by using OSPF cost only.

  Workaround: Use an EXPLICIT ROUTE object or ensure that there are no alternate paths in the network.

- CSCed59978

  Symptoms: A router may crash and reload due to a bus error, and the following error message may appear:

  ```
  Unexpected exception, CPU signal 10
  ```

  Conditions: This symptom is observed on a Cisco router that is running OSPF and that is configured for incremental SPF.

  Workaround: Remove incremental SPF from the router by entering the **router ospf** *process-id* command followed by the **no ospf** command.

- CSCed86069

  Symptoms: A software-forced chunk corruption crash may occur when a MALLOC failure occurs.

  Conditions: This symptom is observed on a Cisco platform that has the **bgp dampening** command enabled.

  Workaround: There is no workaround.

- CSCed93630

  Symptoms: A Cisco router may reload unexpectedly when a **bgp debug** command is enabled.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or Release 12.3T.

Workaround: There is no workaround.

- CSCee11274

  Symptoms: BGP may fail to reestablish a session when you remove a line card, PA, VIP, or module and replace it with a card of a different type. For example, the problem occurs when you remove a 1-port GE line card and replace it with a 3-port GE line card. However, if you replace the 1-port GE line card with another 1-port GE line card (or you just plug the same 1-port GE line card back in the chassis), the problem does not occur.

  Conditions: This symptom is observed when the router one side of the BGP session is configured with the **neighbor** *ip-address* **transport connection-mode active** command and when a line card, PA, VIP, or module is changed on the router at the other side of the BGP session. Furthermore, the router at the other side of the BGP session is configured with the **neighbor** *ip-address* **update-source** *interface* command, and the *interface* argument refers to the interface on the line card, PA, VIP, or module that is changed.

  Workaround: Disable and reenter the **neighbor** *ip-address* **update-source** command.

- CSCee12740

  Symptoms: Traffic through some MPLS TE tunnels may not resume after a forced switch-over has occurred on a router.

  Conditions: This symptom is observed on a router configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels and OSPF.

  Workaround: Perform **clear ip ospf process** on the router.

- CSCee24899

  Symptoms: A router that is configured for multicast routing may reload due to a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software release that contains the fix for CSCec80252. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec80252. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCee35125

  Symptoms: A Cisco router may crash when you enter the **clear ip route *** command.

  Conditions: This symptom is observed when the routing table has a default route.

  Workaround: There is no workaround.

- CSCee36622

  Symptoms: ABRs may continue to generate summary LSA(s) for obsolete non-backbone intra-area route(s).

  Conditions: This symptom occurs under the following conditions:

  1. The ABR (call ABR X) has at least one non-backbone area (call area X) in common with one or more additional ABRs.
  2. The ABRs are generating summary LSAs, on behalf of the Area X's two or more intra-area routes, into the backbone area and other areas. The two intra-area routes must be advertised as stub links from two different routers; i.e., one from ABR X, and the other from another router belonging to Area X.

3. The summary LSA IDs for the intra-area routes above, when ORed with the host bits of the corresponding masks, yield identical LSA IDs.

   For example, 10.10.10.128/25 and 10.10.10.0/24 yield identical LSA IDs when the network address is logically ORed with the host bits; i.e.,

   ```
   10.10.10.128 | 0.0.0.127 = 10.10.10.255
   10.10.10.0   | 0.0.0.255 = 10.10.10.255
   ```

Workaround: Perform the **clear ip ospf proc** command on all ABRs containing the obsolete LSAs.

- CSCee36721

  Symptoms: An OSPF Designated Router (DR) may fail to regenerate the network LSA when you reload the router.

  Conditions: This symptom is observed on a Cisco router that functions as a DR for an OSPF interface when another interface with the same interface address is present in the area but is in a shut down state.

  Workaround: Remove the duplicate interface address and enter the **clear ip ospf process** command.

- CSCee40207

  Symptoms: The BGP Open processes may hold more and more memory, may cause a memory leak, may finally run out of memory, and may cause a Malloc Failure error.

  Conditions: This symptom is observed when there are BGP neighbors stuck in the active state (that is, a BGP neighbor is configured but the peer address is not reachable) and when some NSF/SSO RP switchovers occur and the standby becomes active.

  Workaround: Shut down the neighbors that are not used.

  Further Problem Description: When the memory leak occurs, 1 Kb of memory leaks every two minutes for each BGP neighbor that is not up.

- CSCee41172

  Symptoms: The **maximum-paths import** *number-of-paths* command enables a VRF to import additional paths in addition to the bestpath. If the original path of the import path is withdrawn, wrong import paths may be purged. This situation may cause traffic disruption up to 15 seconds.

  Conditions: This symptom is observed when the original path of the best import path is withdrawn and the import path is at the end of the path list (that is, the one learned the very first). In this situation, all import paths that are derived from other paths may be purged as well. If the imported net has only import paths, the net may not be reachable until other paths are reimported.

  Workaround: Ensure that the import path is at the top of the path list or use the same route descriptor (RD) for all import paths.

- CSCee42285

  Symptoms: Non-EIGRP originated routes are not supported. Furthermore, when a route is injected into mp-BGP from a connected, static, or any other IGP on the remote PE router where the same prefix is also learned via EIGRP (when a backdoor exists for that site), the route may constantly flap between EIGRP and BGP.

  Conditions: These symptoms are observed when the EIGRP MPLS VPN PE-CE SoO feature is configured.

  Workaround: Only inject EIGRP routes into mp-BGP for sites with a backdoor.

- CSCee43166

  Symptoms: The BGP inbound update processing becomes slow and a high CPU utilization occurs for a long time.

Conditions: This symptom is observed when a large number of VRFs (more than 200) and prefixes (more than 220,000) are configured.

Workaround: There is no workaround.

- CSCee59315

  Symptoms: A BGP VPNv4 table may contain paths that may be imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix.

  An example of a path from a deleted BGP table entry is as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 52
Paths: (1 available, best #1, table vpn2)
  Advertised to non peer-group peers:
  10.4.1.2
  2 100, imported path from 2829:2829:185404173:11.13.11.13/-53
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:3
```

  The entry that this path is imported from has been removed from the table and its memory contents contain an incorrect pattern. When the incorrect pattern is displayed as a prefix, it appear as "2829:2829:185404173:11.13.11.13/-53".

  A mismatched prefix appears as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 54
Paths: (2 available, best #1, table vpn2)
Flag: 0x820
  Advertised to non peer-group peers:
  10.10.10.10 10.20.20.20
  2
    10.4.1.2 from 10.4.1.2 (10.4.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:2
  2 100, imported path from 200:2:172.16.0.0/24
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external
      Extended Community: RT:1:3
```

  This BGP VPNv4 table entry is for prefix 192.168.0.0/32 but it shows that a path is imported from 172.16.0.0/24. This situation occurs when a path has a link to a deleted BGP table entry, and then the memory for the deleted entry is reused for a new table entry of which the prefix may not match with the importing entry.

  Conditions: These symptoms are observed when you enter the **maximum-paths import** *number* command in router BGP address-family IPv4 VRF mode. The *number* argument indicates the number of paths to import from one VRF to another.

  Workaround: Remove the **maximum-paths import** *number* command from the router BGP address-family IPv4 VRF mode.

- CSCee65066

  Symptoms: The CISCO-PIM-MIB trap ciscoPimInvalidJoinPrune is supposed to contain the following varbinds:

  ```
  1.3.6.1.4.1.9.9.184.1.1.4 - cpimLastErrorOriginType 1.3.6.1.4.1.9.9.184.1.1.5 -
  1.3.6.1.4.1.9.9.184.1.1.4 - cpimLastErrorOriginType
   1.3.6.1.4.1.9.9.184.1.1.5 - cpimLastErrorOrigin
   1.3.6.1.4.1.9.9.184.1.1.6 - cpimLastErrorGroupType
   1.3.6.1.4.1.9.9.184.1.1.7 - cpimLastErrorGroup
   1.3.6.1.4.1.9.9.184.1.1.8 - cpimLastErrorRPType
   1.3.6.1.4.1.9.9.184.1.1.9 - cpimLastErrorRP
   1.3.6.1.4.1.9.9.184.1.1.2 - cpimInvalidJoinPruneMsgsRcvd
  ```

  However, when the trap is sent, a wrong OID is used for the cpimInvalidJoinPruneMsgsRcvd.

  From a sniffer trace, the following varbind is seen: 1.3.6.1.4.1.9.9.184.2.0.5.0. The actual value sent is correct, though.

  Similarly, another CISCO-PIM-MIB trap, ciscoPimInvalidRegister, has the wrong varbind for cpimInvalidRegisterMsgsRcvd. However the value sent is correct in this case too.

  Conditions: This symptom is platform-independent and software-independent. Note that the actual value that is sent in the wrong OID for cpimInvalidJoinPruneMsgsRcvd or cpimInvalidRegisterMsgsRcvd is correct. However, this situation causes confusion on the traps receiver side because the receiver cannot decode the traps correctly.

  Workaround: There is no workaround.

- CSCee67450

  A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the **bgp log-neighbor-changes** command configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the **show ip bgp neighbors** command or running the **debug ip bgp** *neighbor* **updates** command for a configured BGP neighbor.

  Cisco has made free software available to address this problem.

  For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

- CSCee69396

  Symptoms: A Cisco 10000 series router that is running Cisco IOS Release 12.0(25)SX6 notices a large increase of at least 15% in the CPU usage in the “BGP Router” process when upgraded from Cisco IOS Release 12.0(23)SX5. This occurs under certain conditions where there are a very large number of BGP neighbors in a PE-CE scenario. During the steady state after BGP router convergence, there needs to be a constant churn in the updates with addition/withdrawal of the routes from the neighbor BGP peers.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.0(25)SX6. All versions starting from Cisco IOS Release 12.0(25)SX to Release 12.0(25)SX6 are affected by this problem.

Workaround: Configure the neighbors by grouping into sets or peer-groups, in which a few of the neighbors in each set share similar outbound policy. Each set will fall into a separate update group or peergroup.

- CSCee83549

  Symptoms: When multipath is configured, one of the paths may have an inconsistent (old) label, causing only one path to be operational.

  Conditions: This symptom is observed when BGP does not update the outlabel information in the TFIB and for CEF.

  Workaround: Clear or readvertise the route that is inoperational.

- CSCee89438

  Symptoms: An MSDP enabled RP does not build an (S,G) state from its SA cache when it should do so. Depending on the topology and if an SPT threshold is configured as infinite, this situation may result in a multicast forwarding interruption of up to 2 minutes.

  Conditions: This symptom is observed when the RP for a group fails and an incoming (*,G) join message is received.

  MSDP should create an (S,G) state from its SA cache. However, this is done before the (*,G) olist is populated; because of the (*,G) NULL olist, MSDP does not install an (S,G) state.

  Workaround: Enter the **clear ip mroute *** command on all first-hop routers to the source to enable the FHR to register immediately when the next packet creates an (S,G) state.

- CSCef00535

  Symptoms: An OSPF router may reload unexpectedly.

  Conditions: This symptom is observed after a neighbor has performed a switchover.

  Workaround: Disable LLS under the OSPF process on the router by entering the **no capability LLS** command or disable OSPF NSF under the OSPF process on the neighbor by entering the **no nsf** command.

- CSCef17311

  Symptoms: An %ALIGN-3-SPURIOUS error message and a traceback may be generated when you configure BGP and MPLS VPN.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(9.10)T but may also occur in other releases such as Release 12.0 S and Release 12.2 S.

  Workaround: There is no workaround

- CSCin65241

  Symptoms: ISIS redistribute commands are not synced to the standby RP. The routes dependent on these commands will fail after switchover.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

ISO CLNS

- CSCee54672

  Symptoms: The redistribution of routes from L1 into L2 or/and from L2 into L1 may not occur properly, and a learned IS-IS prefix may be missing.

Conditions: This symptom is observed under the following conditions:

- There are multiple paths to reach the same prefixes.
- One source LSP removes a prefix and another LSP adds the same prefix, while both paths between the prefix and the LSPs are of equal cost.

Workaround: Enter the **clear isis *** or the **clear ip route *** command to restore the prefix. However, doing so clears all the routes and recalculates them again, which is a disruptive action.

Miscellaneous

- CSCdx59158

  Symptoms: An active Route Processor (RP) sets the link correctly to the "down" state, but the standby RP fails to set the link correctly.

  Conditions: This symptom is observed on a Cisco 10000 series when the far end causes the link state to flap from "up" to "down." However, the symptom is not platform-specific and may also occur on other platforms that have dual RPs.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCea28043

  Symptoms: IP commands that are sent in the Cisco Networking Services (CNS) config-changed event output may contain an extra **ip** prefix.

  Conditions: This symptom is observed on a Cisco router when you enter both **ip** global configuration commands and the **cns config notify** *diff* global configuration command to capture commands that change configuration for the config-changed event output.

  Workaround: Enter the *all* keyword in the **cns config notify** global configuration command. This workaround is not valid when the only changes in the configuration occur in the config-changed event output.

- CSCea57710

  Symptoms: A Cisco router may log the following traceback error:

  ```
  %ATMPA-3-BADPARTICLE: Switch1: bad rx particle 0x61CA8040 flags 0x00000001 index 9937
  Traceback= 6007968C 6008F404 60E844F0 60E815F4 60D80BF4 60D8E8A4 6009CF94 600B56EC
  ```

  Conditions: This symptom occurs in the following configuration:

  - A total of 1000 Virtual Private Network (VPN) routing/forwarding (VRF) interfaces are enabled on each RPM-PR.
  - About 98,000 VPN routes have permanent virtual circuits (PVCs).
  - Cell-based Multiprotocol Label Switching (MPLS) is configured for Label Switch Controller (LSC) hot redundancy.
  - Each RPM-PR has 500 external Border Gateway Protocol (EBGP) sessions.
  - The VPN prefixes are advertised with /24(90%) and /30(10%) subnets.

- CSCeb52330

  This caveat consists of two symptoms, two conditions, and two workarounds.

  1. Symptom 1: The interface commands in the CNS configuration notify changed message contain unexpected data.

Condition 1: This symptom is observed when you configure the CNS **cns config notify** *diff* global configuration command and you configure **interface** global configuration commands on the Cisco IOS device.

Workaround 1: There is no workaround if only the changes in the configuration are expected in the CNS configuration notify changed message.

Alternate Workaround 1: Specify the *all* option for the cns config notify global configuration command.

2. Symptom 2: Once the **cns config notify** global configuration command is configured, the router may not detect a newly created interface.

   Condition 2: This symptom is observed when the *diff* option in the **cns config notify** global configuration command is selected and a new dynamic interface is created.

   Workaround 2: There is no workaround.

- CSCec11645

  Symptoms: VIP crashes with DMA Receive error.

  Conditions: This symptom can occur when doing xconnect hairpinning of two interfaces on the same VIP.

  Workaround: There is no workaround.

- CSCec15517

  Symptoms: A Cisco router may reload when you enter the **show policy-map interface** command in one router session while deleting the sub-interface on which the policy is attached from another session.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Frame Relay permanent virtual circuit (PVC) policy.

  Workaround: There is no workaround.

- CSCec77049

  Symptoms: The adjacency table is not retained after an RP switchover.

  Conditions: This symptom occurs with a 4-port Ethernet PA inside a VIP4-80 on an RSP 16.

  Workaround: Clear the adjacency table with the **clear adjacency** command after the Stateful Switchover (SSO).

- CSCec82589

  Symptoms: After entering a **no hw-module slot** command on the primary CSC, an Engine 0 OC-12 (channelized to DS3) line card may be come inoperable.

  Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(24)S.

  Workaround: Use the **microcode reload** global configuration command to reload the line card.

- CSCec87006

  Symptoms: A Multilink PPP (MLP) interface on an Engine 3 CHoC12/T1 line card fails to accept an MQC policy that has a police CIR rate of more than 1536000 bps on the priority queue, even when the MLP interface has a bandwidth of 12288 kbps.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed02844

  Symptoms: IPv6 adjacencies may appear as incomplete, and connectivity may be broken. This situation occurs at random times and is not associated with any event in particular. IPv4 adjacencies may appear as incomplete but recover within a minute.

  Conditions: This symptom is observed on a Cisco IOS-based router when you enter the **clear adjacency** command.

  Workaround: To restore the correct state of the adjacency, enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed08168

  Symptoms: No SNMP linkup or linkdown trap is generated for a 1CHOC12/4CHSTM1 SONET layer when a controller goes up and down.

  Conditions: This symptom is observed when monitoring a SNMP linkup or linkdown trap for a 1CHOC12/4CHSTM1 SONET layer.

  Workaround: Monitor the controller status using the **show controller sonet** command.

- CSCed16318

  Symptoms: When changing the MTU on an Engine 2 3-port 1GE line card, the line card may reload.

  Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(26)S.

  Workaround: Ensure there is no traffic going through the Engine 2 3-port 1GE line card when attempting to change the MTU.

- CSCed22303

  Symptoms: The interface on an Engine 3 line card is stuck after hours of testing. When incoming packets are ignored, PPP does not go up.

  Conditions: This symptom is observed on Cisco 12000 series router after hours of testing with an attenuator.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed35964

  Symptoms: Interoperating problems may occur with a particular third-party vendor 48 MB flash card, and a router may not be able to read the flash card with “bad majic” and “-13 open file” error messages.

  Conditions: This symptom is observed in the following two scenarios:

  – Scenario 1: If the flash card is formatted on one router and then inserted in another router, the boot image and Cisco IOS image can be read from the flash card until you reload the router. After the router is reloaded, “bad majic” and “-13 open file” error messages occur.

  – Scenario 2: When you remove the first large file from the flash card (irrespective of its position on the flash card and irrespective of whether or not the file is a Cisco IOS file) and you reload the router, “bad majic” and “- 13 open file” error messages occur, and the router may enter a continuous loop. The symptom occurs with the removal of a file that is 12 MB or 14 MB but does not occur with the removal of a file of 4 MB.

  Workaround: There is no workaround.

- CSCed54080

  Symptoms: Per-VPN per-destination loadbalancing does not operate correctly on an Engine 2 or 4+ and there seems to be loadsharing only on BGP nexthop.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S4.

  Workaround: The **clear ip route vrf** *vrf-name* command invokes a recalculation of the hashes. Also, the **clear ip bgp** *neighbor* **soft** command (can) reassign(s) new labels and respread(s) the load. These commands may impact service by stopping traffic forwarding.

- CSCed55201

  Symptoms: A serial interface may stop transmitting, and the following error message may be generated:

  ```
  %RSP-3-RESTART: interface Serial1/0/2, not transmitting
  -Traceback= 403D8D88 403E2830 4036B72C 4036B718
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an 8-port serial V.35 port adapter (PA-8T-V35).

  Workaround for HDLC interfaces: Disable CDP, the passive interface, and the outbound IP ACL.

  Workaround for Frame Relay interfaces: Disable CDP, the passive interface, the outbound IP ACL, and LMI.

- CSCed57925

  Symptoms: The cisco.mgmt.cns.config-changed event message is not generated when **atm pvc** CLIs are configured.

  Conditions: This may occur when the CNS configuration notify agent is configured by the **cns config notify** command and **atm pvc** CLIs are configured.

  Workaround: There is no workaround.

- CSCed63357

  This caveat consists, of six separate symptoms, conditions, and workaround, of which the first three apply to all Cisco IOS releases and the last three apply only to Cisco IOS Release 12.3 T:

  1) Symptoms: There are three symptoms:

  – There may be a inconsistent or duplicate display of files between the **show disk***slot-number* and **dir disk***slot-number* commands.

  – When a file is deleted from the CLI, the file may be deleted but a “No such file” message may be printed.

  – One cluster may leak. Entering the **fsck** command truncates the original file and creates an orphan file for the leaked cluster.

  Conditions: This symptom is observed when an application creates or opens a file without the “O_TRUNC:” mode, as in the following example:

  ```
  show version | append disk#:

  Router#conf t
  Enter configuration commands, one per line. End with CNTL/Z.
  Router(config)#vtp file new
  Setting device to store VLAN database at filename new.
  Router(config)#^Z
  ```

  Workaround: There is no workaround.

  2) Symptoms: The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information (such as inconsistent file sizes) when multiple images are copied.

Conditions: This symptom is observed when you make two copies of the image file to the disk by using two vtys and by entering the **dir disk***slot-number* command at the same time.

Workaround: Do not enter the **show disk***slot-number* and **dir disk***slot-number* commands when multiple images are being copied.

3) Symptoms: There are two symptoms:

- The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
- Entering the **fsck** command may delete or truncate the valid files or create an orphan file for an unused cluster.

Conditions: This symptom is observed when you rename a directory that consists of many subdirectories or files.

Workaround: Reload the router.

4) Symptoms: There are two symptoms:

- There may be a duplicate entry for each file when you enter the **show disk***slot-number* command.
- An snmpGet on a ciscoFlashFileSize object may enter a loop.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T after the router boots up.

Workaround: There is no workaround.

5) Symptoms: There are two symptoms:

- The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
- Entering the **fsck** command may delete or truncate the original file.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T when an application or a CLI command overwrites a file on the disk.

Workaround: Reload the router.

6) Symptoms: A router that runs Cisco IOS Release 12.3 T crashes.

Conditions: This symptom is observed when an application creates or opens a file without the "O_TRUNC" mode and attempts to delete the file, as in the following example:

```
show version | append disk0:redirect.out" and issuing
delete disk0:disk0:redirect.out
```

Workaround: Reload the router and delete the file.

- CSCed63508

  Symptoms: Up to 10 percent of packets that are larger than 1496 bytes are dropped when passing through an Engine 3 4-port GE line card (4GE-SFP-LC).

  Conditions: This symptom is observed on a Cisco 12000 series when the line card is used for both the ingress and egress traffic flow. This situation occurs when SNF is configured on the egress interface of the affected line card by entering the **ip route-cache flow sampled output** command.

  Workaround: Increase the MTU on any interface of the Engine 4-port GE line card to 1530 bytes to enable the buffer resources of the line card to be initialized with a larger size.

Alternate Workaround: Decrease the rate of packets drops by increasing the sampling period. For example, when you enter the **ip flow-sampling-mode packet-interval 10** command, up to 10 percent of packets that are larger than 1496 bytes are dropped. However, when you enter the **ip flow-sampling-mode packet-interval 1000** command, only 0.1 percent of packets that are larger than 1496 bytes are dropped.

- CSCed64702

  Symptoms: On a Cisco 10000 series, the PXF information may not be correctly updated from the RP after a route change, causing packets to be sent untagged even though the RP shows that the packets should be sent as tagged.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(26)S.

  Workaround: Enter the **clear isis *** command or enter the **shutdown** command followed by the **no shutdown** command on the interface towards the MPLS cloud.

- CSCed67734

  Symptoms: Packet processing at the remote end of a link may fail.

  Conditions: This symptom is observed when a service policy that includes the **set atm-clp** command is enabled on an output interface via the **service-policy output** command; the platform that links to this output interface at the remote end drops the packets.

  Workaround: Remove the **set atm-clp** command from the service policy on the output interface.

- CSCed69856

  Symptoms: A Cisco 10000 series router may crash when access control lists (ACLs) are displayed.

  Conditions: The symptom is observed when ACLS are displayed by entering the **show access-list** command just after an ACL has been added, deleted or modified. The probability of the crash increases with the size of the ACL and with the number of times it is used (for example, in route maps).

  Workaround: Wait for a few minutes after modifying the ACL. For large size ACLs (with hundreds of entries) that is used many times you may have to wait between 5 and 10 minutes.

- CSCed72686

  Symptoms: An ACL applied to an ATM subinterface (RFC1483) may not work after a PRE switchover.

  Conditions: This problem is observed on a Cisco 10008 router with PRE2.

  Workaround: Deconfigure and configure again the access list that is not working.

- CSCed74917

  Symptoms: An ACL applied to a subinterface may becomes active on the main interface, without showing this in the configuration.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S2.

  Workaround: Do not apply the ACL to the subinterface.

- CSCed74933

  Symptoms: A Cisco 12000 series may exhibit high CPU utilization in the “Per-Second Job” process.

  Conditions: This symptom is observed on a Cisco 12012 router that has a GRP and that is running Cisco IOS Release 12.0(26)S1 with 255 class maps applied to a 4-port ISE Gigabit Ethernet line card. However, the symptom is release- and platform-independent.

Workaround: Reduce the number of applied class maps.

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

  Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

  Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- CSCed76910

  Symptoms: A CHOC12DS1 line card does not support a sufficient number of BERT patterns.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: There is no workaround.

- CSCed82592

  Symptoms: A PXF engine on a Cisco 10000 series may unexpectedly crash and then the router may crash.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(23)S5.

  Workaround: There is no workaround.

- CSCed82964

  Symptoms: L2 loadbalancing might be affected on an egress link bundle.

  Conditions: This symptom is observed a Cisco 12000 series when the ingress interface is a regular Engine 2 interface and when the member interfaces in the bundle are toggled.

  Workaround: Enter the config mode of the port channel and exit.

- CSCed88286

  Symptoms: Layer 3 connectivity may be lost after toggling CEF on a provider edge router.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2 S in an ATM/Ethernet VLAN L2 interworking configuration.

  Workaround: There is no workaround.

- CSCed93593

  Symptoms: The **cisco.mgmt.cns.config-changed** event message contains invalid <changeItem> information.

```
Example: for:  (config)#policy-map TEST2
               (config-pmap)#class m_new
               (config-pmap-c)#shape peak 8010
               (config-pmap-c)#priority
               (config-pmap-c)#exit
               (config-pmap)#desc TESTTEST
               (config-pmap)#exit
The 4th changeItem is: Context:    <empty>
                          EnteredCmd: exit
```

```
NewConfig#: <empty>
OldConfig#:
            !
            MyPolicy
            test
            TEST2
            description TESTTEST
            class m_new
            shape peak 8010
            priority
```

Conditions: This may occur when the CNS configuration notify agent is configured by the **cns config notify** configuration command and policy-map CLI is configured on the Cisco IOS device.

Workaround: There is no workaround.

- CSCed95753

  Symptoms: A GRE tunnel may not work on a PE router.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(25)S or a later release.

  Workaround: There is no workaround.

- CSCee01931

  Symptoms: A router may crash when you enter the **fair-queue** command on the interface of a PA-MC-STM-1 port adapter.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S when the interface has the **rate-limit output** command enabled.

  Workaround: There is no workaround.

- CSCee04454

  Symptoms: A Cisco 10000 series router reloads unexpectedly as ATM VCs are coming up.

  Conditions: This symptom is believed to occur only when ACLs are applied on ATM interfaces, and, only rarely then, on images that contain the CSCed72686 fix.

  Workaround: There is no workaround.

- CSCee13932

  Symptoms: Cisco target FEC stack TLVs may not interoperate with those of third-party vendors.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(27)S or Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCee14817

  Symptoms: HSRP over the VRF is not working after following these steps:

  1. PE router 1 is the active HSRP router and a redundancy forced switchover occurs on PE router 2 (standby HSRP VPN) with SSO configured.
  2. You enter the **shutdown** command on the GE subinterface of PE router 1.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S3, that has a PRP and 4-port GE ISE line cards, and that functions as a PE router.

  Workaround: Enter the **standby use-bia** command or use RPR+ instead of SSO.

- CSCee14840

  Symptoms: A Cisco 12000 series running Cisco IOS Release 12.0(26)S1 may advertise erroneous IPv6 networks when configured for both 6PE and Route Reflector operation.

  Conditions: This symptom is observed on a network in which 6PE is implemented on an existing dual-stack (IPv4 and IPv6) configuration.

  Workaround: There is no workaround.

- CSCee16725

  Symptoms: MPLS VPN VRF labels fail to be updated onto core-facing line cards such that the VPN traffic entering the core-facing line cards is punted to the RP.

  Conditions: This symptom is observed in a setup with two parallel paths between a PE router and a CE router that run Cisco IOS Release 12.0 S. There are around 10,000 VRF routes advertised through both the eBGP sessions that are established between the PE router and the CE router. When the link flaps, the next hop of all the BGP routes changes to the next hop via the other link. When this situation occurs, the core-facing line cards may miss the label forwarding entry for some of the VPN prefixes.

  Workaround: To recover from the problem after it has occurred, enter the **clear cef linecard** command on the affected core-facing line card.

  To avoid the problem from occurring, do not redistribute the PE-CE link subnet into BGP.

- CSCee18889

  Symptoms: If link bundling is configured on any line card in the router and the link bundle is loaded onto an Engine 2 line card that has VPN on FR subinterfaces and that is processing traffic, the Engine 2 line card may reload.

  Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCee22450

  Symptoms: A subinterface on a Cisco 10000 series may drop packets because of unicast RPF check failures, even though the interface is not configured with uRPF.

  Conditions: This symptom is observed on an ATM interface with several subinterfaces when there is at least one subinterface that has uRPF configured. Disabling uRPF on the subinterface still leaves uRPF enabled, even though the CLI indicates it is not enabled. This may also occur with Frame Relay subinterfaces.

  Workaround: Select a subinterface that has uRPF configured, then deconfigure and reconfigure it. This updates all subinterfaces on the interface in such a way that uRPF is correctly enabled or disabled.

- CSCee22810

  Symptoms: On a Cisco 7500 series, all PVCs may suddenly enter the down state and remain in this state for about two minutes before they come back up. During the DLCI down state, the subinterface does not go down and no notifications are observed in the message log.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RPS4+ or an RSP8 and that runs the rsp-jsv-mz image of Cisco IOS Release 12.2(12i). In addition, the router is configured with an 8-port serial port adapter and an HSSI port adapter, is configured for Frame Relay, and has more than 450 PVCs/DLCIs. Note that the symptom may be platform-independent and may also occur on other Cisco platforms in a similar configuration.

  Workaround: There is no workaround.

- CSCee22933

  Symptoms: CBR-type or VBR-type VP cell-relay or cell-packing AToM VCs may not be able to retain their bandwidth to the configured CBR or VBR shaping rate. This situation persists even when the total shaping rate of the VPs and VCs is far below the physical bandwidth of the interface.

  Conditions: This symptom is observed when there are many other cell-relay or cell-packing AToM VCs configured.

  Workaround: There is no workaround.

- CSCee23607

  Symptoms: An L2tpv3 tunnel does not come up.

  Conditions: This problem can be seen in an ATM-FR interworking scenario.

  Workaround: There is no workaround.

- CSCee24349

  Symptoms: A Cisco 7500 series cannot boot when there are more than 256 different policy maps attached as service policies on the router.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 but may also occur in Release 12.2 S.

  Workaround: Do not use more than 256 service policies.

- CSCee25588

  Symptoms: A 12000 series Engine 2 line card may not accept a “tx-cos” configuration.

  Conditions: This symptom is observed if the router previously had an Engine 4+ line card in the same slot and this Engine 4+ line card was configured with an output service policy.

  Workaround: Reload the router.

- CSCee26497

  Symptoms: The service-policy does not get attached.

  Conditions: This symptom occurs when the **atm pvc subinterface** command is configured with UBR pvc and a service- policy with police percent configuration is attached to the PVC.

  Workaround: Use vbr or abr on the PVC or specify police rate in bps instead of percent.

- CSCee27276

  Symptoms: A router shows a constant increase in the holding memory for the L2TP Daemon process.

  Conditions: This symptom is observed when invalid L2PTv3 control packets are sent from a peer router. Invalid packets means packets without all the mandatory attribute value pairs.

  Workaround: There is no workaround.

- CSCee27396

  Symptoms: High CPU usage of greater than 90 percent occurs in the CEF Scanner process on all line cards and TFIB-7-SCANSABORTED errors occur when you configure a link bundle.

  Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(26)S1 when the bundle is configured on interfaces gig2/2 and gig6/2. (A 4-port Gigabit Ethernet ISE line card is installed in slot 2 and slot 6.) The link bundle terminates on a third-party vendor switch.

  Workaround: Remove the link bundle and use only one of the Gigabit Ethernet ports.

- CSCee28481

  Symptoms: After working fine for sometime, a 4-port OC-12 ATM line card stops forwarding unicast packets to the RP, and none of the unicast traffic that is sourced from or destined to the RP via the 4-port OC-12 ATM line card goes through. Unicast traffic to the 4-port OC-12 ATM line card interfaces fails too.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(21)ST7 when MPLS is enabled on the line card. IP traffic and IS-IS traffic that pass through the router are not affected. To recover the line card, reset the line card.

  Workaround: There is no workaround.

- CSCee28754

  Symptoms: GE interfaces on an EPA-GE/FE-BBRD line card may drop tag packets.

  Conditions: The problem is reported on a Cisco 12000 series running Cisco IOS Release 12.0(23)S5 only when you perform an OIR of an EPA-GE/FE-BBRD to install or remove additional EPA-3GE-SX/LH line cards.

  Workaround: Perform a second OIR of the line card.

- CSCee29196

  Symptoms: When a Cisco 10000 series does not have a specific route for both end points of a voice connection, the Cisco 10000 series duplicates one-way audio only for the specific route that populates its routing table, not for the end point that uses the default route from the routing table.

  Conditions: This symptom is observed on a Cisco 10000 series that is runs Cisco IOS Release 12.0(25)S3 and that is configured with a PRE-1.

  Workaround: There is no workaround.

- CSCee30089

  Symptoms: If a multilink interface loses members of the bundle, or if you enter the **shutdown** command followed by the **no shutdown** command on a multilink interface, or if the router reloads, the bandwidth that is allocated for non-real time classes can be allocated incorrectly. The sum of the bandwidth that is allocated for non-real time classes and the bandwidth that is specified by the **police** *bps* command for real time traffic may exceed the actual bandwidth of a multilink interface.

  Conditions: This symptom is observed on a Cisco 10000 series running Cisco IOS Release 12.0(27)S1 that has the **service-policy out** command enabled on a multilink interface. The service policy consists of a real-time class and several classes with reserved bandwidth The real-time class is configured with the **priority** command and the **police** *bps* command. Other classes are configured with the **bandwidth** *bandwidth-kbps* command.

  The bandwidth that is allocated for non-priority traffic should take into account the bandwidth that is reserved by the **police** *bps* command for the real-time class.

  Workaround: Remove and reapply the **service-policy out** command to the multilink interface.

- CSCee30116

  Symptoms: CNS config notify events may stop coming.

  Conditions: This symptom is observed when the **cns config notify diff** command is enabled and when other CNS configuration agents are configured.

  Workaround: Enter the **no cns config notify** command followed by the **cns config notify diff** command.

- CSCee30527

  Symptoms: After reloading a Cisco 12000 series, the following message may be seen on an Engine 2 or Engine 3 line card:

  ```
  %MBUS-2-DNLDFAIL: IOS download to slot 7 fail, timeout
  ```

  In some cases this situation may prevent the line card from coming up:

  ```
  %GRP-3-ABANDON_DOWNLOAD: End attempt to start the linecard in slot 7
  ```

  Conditions: This symptom is observed rarely on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: The line card may come up when you reload the router again.

- CSCee31105

  Symptoms: A wrong aggregate NetFlow cache prefix may occur when an extended Deny ACL is configured with AGNF. You are supposed to find one prefix entry in the cache but there are two prefix entries.

  Conditions: This symptom is observed when an extended Deny ACL is configured with AGNF on a Cisco 12000 series Engine 3 16-port OC-3 POS line card.

  Workaround: There is no workaround.

- CSCee31618

  Symptoms: Buffer leakage could occur when a high load of traffic is sent to an interface that has a service policy enabled. This could result in ping failures or very long packet delay.

  Conditions: The problem is observed with an MC-T3+ interface that is configured in unchannelized mode, and the traffic consists only of small packets such a 64-byte packets.

  Workaround: Manually configure the **tx-ring-limit** command to lower the number of packets that can be placed on the transmission ring.

- CSCee32208

  Symptoms: After a circuit bounces, traffic stops being passed on a VC when using a VC bundle. Other VCs on the same subinterface still work. The switch on the other side of the VC does not show any received cells from the VC.

  In addition, the **show atm vc** command does not work because even after the VC is recovered, the command output still does not show any traffic.

  Conditions: These symptoms are observed on a Cisco 12000 series.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected subinterface.

- CSCee32484

  Symptoms: After performing a manual switchover on a dual-RP router that functions in RPR+ or SSO mode, the following error message may be seen on an 8xOC3ATM line card, and the line card may stop forwarding traffic:

  ```
  %QM-4-STUCK: Port 0 Queue mask 0x80
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: Perform a microcode reload on the line card.

- CSCee32921

  Symptoms: Line cards in a Cisco 12000 series dual-RP router running Cisco IOS Release 12.0(28)S may fail when the active RP is reloaded.

Conditions: This symptom is observed when the active RP is reloaded by entering the **microcode reload** command.

Workaround: There is no workaround.

- CSCee34076

  Symptoms: Routes that are removed soon after an SSO switchover occurs may remain in the CEF table.

  Conditions: This symptom is observed when VRFs are configured.

  Workaround: There is no workaround.

- CSCee34094

  Symptoms: A standby RP keeps crashing.

  Conditions: This symptom is observed when both the **snmp-server community** *string* **rw** command and the **snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart** command are configured.

  Workaround: Remove the **snmp-server community** *string* **rw** command from the startup configuration before rebooting the router. When the router has booted, reenter the **snmp-server community** *string* **rw** command.

- CSCee34133

  Symptoms: If CEF fails, you cannot enable CEF IPv6 by entering the **ipv6 cef distributed** command.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCee34474

  Symptoms: The Open Shortest Path First (OSPF) peers were mapped to the wrong subinterfaces.

  Conditions: A High Availability (HA) switch over the ATM interfaces was up and appeared to be operational with OSPF adjacencies formed.

  Workaround: There is no workaround.

- CSCee35185

  Symptoms: After reloading a Cisco platform, one of the RPs may reload, or the following error message may be displayed:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file.
  ```

  Conditions: This symptom may be observed on any Cisco platform that is configured with dual RPs and that supports RPR+.

  Workaround: There is no workaround.

- CSCee35331

  Symptoms: A router may reload if removing the L2TP class is followed by removing the pseudowire class.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.0(28)S when both removals are done in a very short time via an auto test script and when the L2TP sessions are already established. This is a timing related issue. The symptom could also occur in other releases.

  Workaround: Wait at least 1 second before you remove the pseudowire class.

- CSCee35659

  Symptoms: A priority class cannot be configured if the remaining bandwidth is used on the existing classes. Such a service policy is rejected.

  Conditions: This symptom is observed on Cisco 12000 series-ISE based line cards.

  Workaround: Use police actions in the priority class in conjunction with bandwidth percentages on the existing classes.

- CSCee36050

  Symptoms: A VIP crashes with the following error message:

  ```
  VIP-3-SYSTEM_EXCEPTION: VIP System Exception occurred sig=10, code=0x10
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when you re-use a channel group (or subinterface) that was previously configured with a Frame Relay DLCI “set” service policy.

  Workaround: Remove the “set” service-policy before you remove the channel group (or subinterface).

- CSCee38324

  Symptoms: A VIP may crash.

  Conditions: This symptom is observed on a Cisco 7500 series when QoS is configured on the interface of the VIP and traffic is flowing.

  Workaround: There is no workaround.

- CSCee38348

  Symptoms: The SNMP counters and CLI for Frame Relay subinterfaces may be incorrect.

  Conditions: This symptom is observed a Cisco 12000 series with ISE POS line cards.

  Workaround: There is no workaround.

- CSCee38942

  Symptoms: EoMPLS tunnels do not have labels assigned to them, preventing a virtual circuit from coming up.

  Conditions: This symptom is observed when multiple (for example, 1200) EoMPLS tunnels are configured. Only on a few tunnels the symptom may not occur.

  Workaround: There is no workaround.

- CSCee39853

  Symptoms: A Cisco router that is running Cisco IOS Release 12.0(25)SX1 may experience CEF disabling on standby PRE.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(25)SX1. The symptom may also occur in Release 12.0 S.

  Workaround: Reset standby PRE.

- CSCee39854

  Symptoms: A ping or Telnet connection to a connected CE router may fail from a Cisco 12000 series router that functions as a PE router.

  Conditions: This symptom is observed on Cisco 12012 that runs Cisco IOS Release 12.0(21)ST3 or a later release when the router has a 3-port Gigabit Ethernet line card that is configured for dot1q encapsulation on its subinterfaces.

  This symptom occurs because of a misconfiguration on the subinterfaces: when you configure a subinterface with new a VRF without removing the already configured VRF, the symptom occurs.

Workaround: Unconfigure and reconfigure the VRF configuration on the misconfigured subinterfaces.

- CSCee40349

  Symptoms: Cisco 12816 and 12810 routers need to have specific MBSU 5v and on- board 5v thresholds other than the values in the legacy system. Otherwise, there may be error messages in the console logs that complain that the voltages are abnormal.

  Conditions: This symptom is observed on Cisco 128xx series routers.

  Workaround: The **no show environment** command can be configured, but only if this problem is seen.

- CSCee41413

  Symptoms: An active PRE on a Cisco 10000 series may crash.

  Conditions: This symptom is observed when the standby PRE goes down just when the driver of a CHSTM1 or CHOC12 line card attempts to synchronize a linestate message.

  Workaround: Avoid resetting the standby PRE unnecessarily.

- CSCee41544

  Symptoms: If there is sequence number enabled on a PVC and you add a service policy to this PVC, the sequence number configuration is lost.

  Conditions: This symptom is observed when you enable the sequence number configuration and then add a service policy to the same PVC.

  Workaround: After the symptom has occurred, re-add the sequence number configuration to the PVC.

- CSCee41728

  Symptoms: Some voltage threshold levels may not be set correctly and may cause a line card to power down without any warning messages if the voltage drops below 3v. Note: There has been no reports of this happening yet.

  Conditions: This symptom is observed on Cisco 12000 series routers.

  Workaround: The **no show environment** command can be configured, but only if this problem is seen.

- CSCee42198

  Symptoms: Engine 4+ loadsharing does not work correctly in a VPN imposition situation. The problem is not seen with Engines 0, 2 and 3.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S when traffic enters on a VRF interface and is loadshared over four links to the core. Traffic is loadshared over only two of the four links.

  Workaround: Use three-path loadbalancing.

- CSCee42279

  Symptoms: During an L2TPv3 test with a Cisco 12000 series 4-port OC-12 ATM line card, when you bump traffic on more than two ports that process a high rate of traffic, traffic may stop. When this situation occurs, the CPK24 FPGA on the line card generates ingress packet length errors and sometimes SDRAM CRC errors.

  Conditions: This symptom is observed on a 4-port OC-12 ATM line card that is configured for L2TPv3 and that is installed in a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0 S.

Workaround: Reload the line card.

- CSCee43259

  Symptoms: In the case of a Cisco 12000 series router using Supervisor Engine 3 ISE QOC12 ATM card, Route Processor (RP) may hang for about 15-20 minutes when the following two steps are done:

  Conditions:

  - Configure 1K ATM PVCs (1K ATM sub-interfaces) with a class-default (queue-limit) based service-policy configured on all of the PVCs (service-policy should be configured under each PVC to see RP hangs and crash).
  - On removing the above 1k ATM PVCs (sub-interfaces), RP hangs for about 15-20 minutes before the user can regain control.

    The following warning message may show up when deleting the ATM sub-intfs:

    ```
    %WARNING: Features on ATM6/0.1 haven't been removed Please wait for approximately
    ten minutes and retry.

    % Removal of physical interfaces is not permitted.
    ```

  - On adding the 1K sub-intfs again (2nd attempt), RP crashes. This RP crash is reproducible.

  Workaround: There is no workaround.

- CSCee43562

  Symptoms: The feature manager queue on the Route Processor may not drain for 20 minutes after a reload in a scaled environment with 1400 IP and L3VPN connections (subinterfaces). The feature manager pushes ACL and PBR configurations to the IP Services Engine (ISE) line cards for TCAM processing. You can monitor the state of the feature manager queue with the **show fm queue** command.

  Conditions: This symptom is observed on a 12000 series that runs Cisco IOS Release 12.0(28)S and may occur on any ISE line card that uses an associate message in the QoS manager.

  Workaround: There is no workaround.

- CSCee43569

  Symptoms: The TE DB on a tunnel headend may become corrupted.

  Conditions: This symptom is observed on a Cisco router that has MPLS configured.

  Workaround: There is no workaround.

- CSCee43880

  Symptoms: After reloading an E2 16-port OC-3 POS line card that is a member line card of POS channel, the peer POS channel members do not become active members again.

  Conditions: The symptom is observed on a link-bundling interface of a Cisco 12000 series router that runs Cisco IOS Release 12.0 S.

  Workaround: There is no workaround.

- CSCee45099

  Symptoms: A Cisco 12000 series 8-port OC-48 or 2-port OC-192 line card may crash.

  Conditions: This symptom is observed when the line card is configured for MPLS-TE FRR.

  Workaround: There is no workaround.

- CSCee47026

  Symptoms: The ATM HA process may crash.

Conditions: This symptom is observed on a Cisco router that has VCS configured with local switching.

Workaround: There is no workaround.

- CSCee51126

  Symptoms: A Cisco 12000 series may drop 2 to 3 percent of the ping packets that are destined to the router when the input interface is an Engine 4+ line card.

  Conditions: This symptom is observed for ICMP packets on a Cisco 12000 series that is Cisco IOS Release 12.0(26)S1. The symptom may also affect other types of packets.

  Workaround: There is no workaround.

- CSCee51909

  Symptoms: An Engine 3 channelized (OC-48 to DS3) line card that processes traffic crashes.

  Conditions: This symptom is observed when you change the MTU on the E4+ disposition line card.

  Workaround: There is no workaround.

- CSCee52028

  Symptoms: A Cisco 12000 running Cisco IOS Release 12.0(28)S fails to properly apply IPv6 ACLs when the ACLs match packets based on the IPv6 source address.

  Conditions: This symptom exists for all IPv6 ACLs applied on Engine 3 line cards.

  Workaround: There is no workaround.

- CSCee53458

  Symptoms: After you boot a Cisco 12000 series, one of the members of a link bundle that has eight members that are configured on an Engine 2 16-port O-C3 POS line card shows up in both the active and passive lists.

  Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release of Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

  Further Problem Description: Proper functionality is not impacted by this caveat.

- CSCee53472

  Symptoms: Interfaces of a line card may stay in the link down and line down states when you create an initial configuration on a new line card.

  Conditions: This symptom is observed on a Cisco 10000 series when a previously unprovisioned line card is introduced into the system and a new configuration is entered for this line card.

  Workaround: After inserting the new line card, save the configuration and reboot the router.

- CSCee54143

  Symptoms: An E1 port on a PA-MC-8T1 port adapter may stay down after a VIP crash.

  Conditions: This symptom is observed on a Cisco 7513 that is configured with a VIP in which a PA-MC-8T1 port adapter with a channelized E1 (or T1) port is installed in slot 0.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCee54198

  Symptoms: A Cisco 12000 series crashes because of a bus error.

Conditions: This symptom is observed on a Cisco 12016 that runs Cisco IOS Software 12.0(25)S2 when you enter the **hw-module slot 17 shutdown** command to shut down the master scheduler card.

Workaround: Do not shut down the master scheduler card.

- CSCee55457

  Symptoms: When a channel group (for example, channel +1) is removed from a controller, the class-default queue gets stuck on the next time slot/channel.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 24-port channelized E1/T1 line cards and that has a high traffic rate on the removed channel.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCee56199

  Symptoms: An egress IPv6 QoS policy does not work after a Cisco 12000 series reboots.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S when the following conditions are met:

  – An IPv6 ACL is used to match traffic.
  – UDP ACEs are used in the IPv6 ACL.
  – Matching UDP traffic is sent.

  Note that matching TCP traffic works fine.

  Workaround: There is no workaround.

- CSCee56225

  Symptoms: A Cisco router may experience alignment errors involving MPLS and BGP, and the output of the **show alignment** command may show the following information:

```
Total Spurious Accesses 1, Recorded 1
 Address  Count  Traceback
       C      1  0x612EE93C 0x60BD2894 0x60BD2F0C 0x60B8C2DC
```

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS and BGP.

  Workaround: There is no workaround. However, note that the symptoms are of a transient nature and do not affect the functionality of the router.

- CSCee57438

  Symptoms: The second port pair (interface SRP x/1) of an Engine 4+ 4-port OC-48 DPT line card is unable to forward traffic (including pings) at layer 3. The first port is also damaged (interface SRP x/0); a portion of its forwarding capabilities is damaged. The layer 2 SRP protocol operates correctly.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 and does not require any specific trigger: the symptom is always there.

  Workaround: There is no workaround.

- CSCee57485

  Symptoms: There are two symptoms:

  – Packets with explicit null labels may be dropped from an Engine 4+ POS line card.
  – CEF may become disabled on an Engine 4+ POS line card.

  Conditions: These symptoms are observed on a Cisco 12000 series under the following conditions:

  - The router functions as a PE router with the Engine 4+ POS line card facing the core and performing MPLS disposition.
  - VRFs are configured on the router.
  - The Explicit Null feature is enabled on the router.

  Workaround: There is no workaround.

- CSCee58770

  Symptoms: A Cisco router may generate the following error message:

  ```
  %TUN-5-RECURDOWN: Tunnel2 temporarily disabled due to recursive routing
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2 and that is configured with a tunnel services card (TSC) (that is, a 1-port OC-48 POS line card) when MPLS TE tunnels are configured on the router and when static routes are added.

  Workaround: There is no workaround.

- CSCee59106

  Symptoms: The performance of an OC-48 to E3 concatenated or channelized line card may drop from 4 Mpps to 2.84 Mpps when oCAR is enabled in a configuration that includes both the **conform-action** and **exceed-action** keywords and when oCAR is transmitting packets and changing the precedence.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S or an earlier release. However, note that performance drops do not occur in Release 12.0(27)S1.

  Workaround: There is no workaround.

- CSCee59585

  Symptoms: On a Cisco router, the output of the **execute-on slot** *number* **show ip cef** *prefix* command may display the same imposed label twice for a recursive public route.

  Conditions: This symptom is observed on a Cisco platform that supports distributed forwarding such as a Cisco 7500 series or a Cisco 12000 series when the **neighbor** *name* **send-label** command is configured under an IPv4 BGP address family on a VIP or line card and when one of the following actions occurs:

  - You enter the **clear cef linecard** command.
  - You perform an OIR of the VIP or line card.
  - You enter the **no ip cef distributed** command followed by the **ip cef distributed** command.

  The symptom disappears after the affected prefix flaps.

  Workaround: There is no non-impacting workaround, but you can enter the **clear ip route** *prefix* command or reset the BGP peer to solve the problem.

- CSCee63939

  Symptoms: An Engine 6 line card may crash during the MDFS process.

  Conditions: This symptom is observed on a Cisco 12000 series when multicast and unicast traffic are running through the Engine 6 line card.

  Workaround: There is no workaround.

- CSCee65004

  Symptoms: A 1-port 10-Gigabit Ethernet line card (1X10GE-LR-SC) may crash, reporting %TX192-3-CPUIF errors.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 when you shut down the 10GE port of a 4-port 10 Gigabit Ethernet module (WS-X6704-10GE) that is installed in a Cisco 7609 at the other side of the connection.

  Workaround: There is no workaround.

- CSCee66206

  Symptoms: When you boot a Cisco 7200 series that is configured with an NPE-300 or NPE-400 and that runs a c7200-js-mz image, the router may crash with a traceback.

  Conditions: This symptom is observed when the c7200-kboot-mz image is the bootloader and when the router runs Cisco IOS interim Release 12.1(22.3)E1. The symptom may also occur in other releases such as 12.0 S, 12.2 S, and 12.3.

  Workaround: There is no workaround.

- CSCee67207

  Symptoms: A public recursive route is not labeled.

  Conditions: This symptom is observed on a Cisco router that functions as a BGP peer and that has the **neighbor** *name* **send-label** command enabled as part of an IPv4 address family, which is required for Inter-AS configurations. The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

  Workaround: There is no workaround. Note that the symptom does not occur if the **neighbor** *name* **send-label** command is enabled as part of an IPv4 address family VRF.

- CSCee68666

  Symptoms: It may take up to 1 second for a line card to notify the RP about a physical layer failure alarm. This situation prevents fast sub-second IGP convergence.

  Conditions: This symptom is observed in a non-FRR and non-APS configuration.

  Workaround: There is no workaround.

- CSCee69861

  Symptoms: When a host sends a path MTU discovery packet into a L2TPv3 tunnel, a Cisco 10720 returns an ICMP unreachable packet, indicating that the path MTU is “MTU-32byte (L2TPv3 header)-(layer2 header of customer packets),” which is incorrect. This situation causes TCP communications such as FTP or HTTP downloads over the L2TPv3 tunnel to fail. For example, 26 bytes (outer IP + L2TPv3 header sizes) may be missing.

  Conditions: This symptom is observed on a Cisco 10720 that functions as a PE router.

  Workaround: If this is an option, set an MTU with a small size at the server side. If this is not an option, there is no workaround.

- CSCee69887

  Symptoms: A dual SRP ring fails to become active completely due to an is-type mismatch. The output of the **show clns neighbors** command indicates that a certain system interface remains in the “Init” state indefinitely, although the output of the **show ip interface brief** command shows that this interface is up.

  Conditions: This symptom is observed when a dual SRP ring is configured on three routers that run Cisco IOS Release 12.2S. The symptom may also occur in other releases.

Workaround: There is no workaround.

- CSCee70024

  Symptoms: LSP-Ping packets may include a Vendor Enterprise Code TLV Type 5 with a length that is greater than 4 and with Vendor Private Extensions. According to the draft-ietf-mpls-lsp-ping-05.txt IETF draft, the Vendor Enterprise Code TLV Length should always be 4, and the vendor extensions should use a TLV Type that is in the range 64512-65535.

  Conditions: This symptom is observed on a Cisco platform that functions in an MPLS OAM environment.

  Workaround: There is no workaround.

- CSCee70478

  Symptoms: If hardware multicast forwarding is enabled on an Engine 2 line card that is connected to the source of multicast traffic, multicast traffic may not be forwarded after the router has reloaded.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(27)S2.

  Workaround: Remove and reapply hardware multicast forwarding to the line card.

- CSCee71793

  Symptoms: Malformed MPLS echo request packets may cause excessive Route Processor (RP) CPU cycles to be consumed during parsing of malformed TLVs.

  Conditions: This symptom is observed when MPLS echo request packet are decoded and incorrectly parse beyond the packet boundary due to improper bounds checking.

  Workaround: There is no workaround.

- CSCee72027

  Symptoms: WRED does not share WRED labels even when WRED parameters are identical. Because Engine 4 and Engine 4+ line cards have only seven WRED labels, when you configure WRED for all eight IP precedences, the line cards display the following error:

  ```
  % Can not configured WRED, all WRED labels are in use.
  ```

  This situation prevents part of the **precedence** (WRED group) command for the 8th IP precedence from being applied to the interface policy map.

  Conditions: This symptom is observed when you apply a policy map that uses more than seven WRED labels and when WRED labels are not shared.

  Workaround: There is no workaround.

- CSCee72353

  Symptoms: An LDP session over a tunnel interface may drop and not come back up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S when auto-tunnel traffic engineering is configured and when RSVP label distribution and LDP are configured in the MPLS core.

  If the **no mpls ip** command is configured on the physical interface to disable LDP, and RSVP label distribution remains enabled, auto-tunnel traffic engineering fails and you cannot bring the tunnel back up.

  Workaround: Run LDP in the MPLS core for all interfaces that have auto-tunnel traffic engineering configured.

- CSCee73410

  Symptoms: When you enter the **redundancy force-switchover** command, IPC messages and tracebacks may be generated on an Engine 2 3-port GE line card.

  Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S and that has dual PRPs.

  Workaround: There is no workaround.

- CSCee74419

  Symptoms: When L3 VPN routes flap, the PLU utilization on line cards in a PE router may increase to and remain at 99 percent.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S and that functions as a PE router when L3 VPN routes flap in an L3 VPN network that has a large number of VPN routes.

  Workaround: There is no workaround.

- CSCee74886

  Symptoms: After you enter the **microcode reload pxf** command or after a PXF crash occurs, EoMPLS packets that should be encapsulated with EoMPLS encapsulation are treated as if they are normal IP packets, and are likely to be dropped by the router.

  Conditions: This symptom is observed on a Cisco 10720 router when an SRP (sub)interface is used as the EoMPLS backbone interface to transport EoMPLS packets to other EoMPLS PE routers and when the (sub)interface has the **xconnect** *destination-address vc-id* **encapsulation mpls** command enabled.

  Workaround: Remove the **xconnect** *destination-address vc-id* **encapsulation mpls** command from the (sub)interface that connects to a customer device, and reconfigure it on the (sub)interface.

- CSCee75225

  Symptoms: High CPU utilization may cause interfaces to flap, and the following spurious memory access messages may be generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x603C2724 reading 0x194
  %ALIGN-3-TRACE: -Traceback= 603C2724 601D2888 601D40B4 00000000 00000000 00000000
  00000000 00000000
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(23)S when you the **clear cef linecard** command.

  Workaround: There is no workaround.

- CSCee76306

  Symptoms: A Cisco router crashes during a period of high routing protocol activity.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(21)SP or a later release or Release 12.0(22)S or a later release.

  The crash is most likely to occur when the router holds a large number of IPv4 prefixes in its routing table and when there is a lot of turnover in the routing table, that is, prefixes are added and deleted on a rapid basis.

  Workaround: There is no workaround.

- CSCee76476

  Symptoms: A Cisco 12000 series equipped with Engine 4 or Engine 6 line cards may crash because of an unexpected exception to CPU vector 300 when the CISCO-CLASS-BASED-QOS-MIB is queried via SNMP.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or an earlier 12.0 S release.

Workaround: There is no workaround other than excluding the access to the MIB.

- CSCee76995

  Symptoms: A packet becomes corrupted when you ping a POS line card.

  Conditions: This symptom is observed on a Cisco 12000 series Engine 0 4-port OC-3 POS line card. It only affects IOS 12.0(28.3)S.

  Workaround: There is no workaround.

- CSCee77227

  Symptoms: When a channel group is removed and readded to the controller, and then a PRE switchover occurs, the PPP line protocol on the readded channel goes down after a while.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 24-port channelized E1/T1 line cards.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCee77328

  Symptoms: The PXF forwarding engine on a Cisco 10720 may crash after the microcode is reloaded either through a manual reload by entering the **microcode reload pxf** command or after a previous PXF crash. This situation causes multiple PXF crashes.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(26)S or a later 12.0 S release, all of which contain IPv6 PXF packet forwarding functionality, and is most likely to occur while IPv6 packets are passing through the router.

  Workaround: Disable IPv6 functionality or disable PXF by entering the **no service pxf** command.

- CSCee78118

  Symptoms: A line card or port adapter may crash on an MPLS VPN PE router when the customer-facing interfaces are flapped.

  Conditions: This symptom is observed when any of the following conditions are present:

  – eBGP is used as the routing protocol between the PE and CE router, the CE router has the **redistribute connected** command enabled in the BGP configuration, and there are multiple eBGP sessions between the PE and CE router.

  – The connected route for the link between the CE and PE router is learned from another PE router via MP-iBGP. For example, the CE router may be dual-homed and may advertise the connected routes to both PE routers.

  The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

  Workaround: Avoid the above-mentioned conditions. For example, avoid the **redistribute connected** command in the BGP configuration of the CE router.

- CSCee78567

  Symptoms: A temporary counter condition in which you see very large MPLS TE tunnel counter spikes may occur on a Cisco 12000 series. This situation is observed via the SNMP variable IfHCOutOctets (the total number of octets transmitted), via the SNMP variable locIfOutBitsSec (the Cisco 5-minute decaying average), and in the output of the **show interfaces tunnel** *number* privileged EXEC command (observe the elevated output rate).

Conditions: This temporary counter condition is observed only for one or two sample periods and affects the MPLS-TE auto-bandwidth mechanism because the collection timer may be invoked at a time while the counter is at an extreme value. If the auto-bandwidth mechanism collection value is greater than the physical interface capability, the LSP tunnel build fails at the next LSP tunnel build.

Workaround: There is no workaround.

- CSCee79125

  Symptoms: The standby RP may notify client applications about a state-change event even if there is no change in the state.

  Conditions: This symptom is observed on a Cisco 10008 that runs Cisco IOS Release 12.0S. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCee80041

  Symptoms: A line card with an ATM QoS configuration may crash.

  Conditions: This symptom is observed on a Cisco 12406 that runs a Cisco IOS interim release of Release 12.0(29)S. However, this caveat is resolved in Release 12.0(29)S.

  Workaround: There is no workaround.

- CSCee80214

  Symptoms: When you delete shaping by entering the **no shape** *cir* command, shaping seems to be disabled on all interfaces, which can be seen in the output of the **show policy-map interface** *interface-name* command. However, the output of the **show policy-map** *policy-map* command still shows the shape value.

  Conditions: This symptom is observed on Frame Relay subinterfaces on a Cisco 10000 series.

  Workaround: Remove and reconfigure the Frame Relay class on each subinterface or remove the policy map from the map class and reconfigure the policy map.

- CSCee81787

  Symptoms: A VIP crashes with a “DRQ stalled” error message.

  Conditions: This symptom is observed when a switchover occurs on a Cisco 7500 series.

  Workaround: There is no workaround.

- CSCee82088

  Symptoms: The **show controller au-4** command does not show any detail tug groups under the controller.

  Conditions: This symptom is observed on the Cisco 10000 router with a channelized STM-1 linecard.

  Workaround: Issuing the following commands on the router will restore the au-4 controller display.

  ```
  router# config terminal
  router(config)# hw-module slot <slot number> shutdown
  router(config)# no hw-module slot <slot number> shutdown
  router(config)# end
  router#
  ```

- CSCee84933

  Symptoms: A 1-port 10-Gigabit Ethernet line card (1X10GE-LR-SC) may crash, reporting a stack trace pointing to the optics interrupt handler.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 when you shut down the 10GE port of a 4-port 10 Gigabit Ethernet module (WS-X6704-10GE) that is installed in a Cisco 7609 at the other side of the connection.

Workaround: There is no workaround.

- CSCee90155

  Symptoms: A TLU memory leak occurs on an Engine 3 line card that has aggregate IPv6 labels when the associated IPv6 route is flapped or changed.

  Conditions: This symptom is observed when you inject static routes that point out of a Gigabit Ethernet (GE) interface of a 4-port GE ISE line card and when the GE interface is flapped.

  Depending on the number of aggregate IPv6 labels, the TLU memory leak can be either service-impacting or very minor.

  Workaround: There is no workaround.

- CSCee90295

  Symptoms: A Cisco 12000 series may reload when you configure a large number of class maps.

  Conditions: This symptom is observed on a Cisco 12816 that has a PRP and that runs Cisco IOS Release 12.0(28)S.

  Workaround: Configure a maximum of 255 classes per parent policy map.

- CSCee90552

  Symptoms: When you send an SNMP query to poll the CBQOS MIB, high CPU utilization may occur. Depending on number of service policies attached, the CPU utilization may reach 100 percent, causing many different negative effects to occur: the Telnet connection may go down, LDP may go down, and in some cases the router may crash.

  Conditions: This symptom most likely occurs when the unsupported cbQosREDClassStats objects are polled and when there are about 1000 QoS policy attachment configured.

  Workaround: The potential workarounds include the following:

  - Reduce the number of QoS policy attachments.
  - Avoid polling the unsupported stats table(s).
  - Reduce the polling frequency.

- CSCee90590

  Symptoms: A 6-port OC-3 POS line card (ESR-6OC-3/P-SMI=) may go down unexpectedly, and the following error messages may be logged (assuming that the line card is installed in slot 6 of the router):

  ```
  IPCOIR-4-REPEATMSG: IPC handle already exists for 6/0
  IPCOIR-2-CARD_UP_DOWN: Card in slot 6/0 is down. Notifying 6oc3pos-1 driver.
  C10K_ALARM-6-INFO: ASSERT CRITICAL slot 6 Card Stopped Responding OIR Alarm -
  subslot 0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S2 in a dual-PRE configuration when the CPU utilization on the active PRE is high. The symptom may also occur in other 12.0 S releases.

  Workaround: There is no workaround.

- CSCee90893

  Symptoms: An RP may crash if a policy map matches a QoS group value that is greater than seven.

Conditions: This symptom is observed on an interface of a Cisco 12000 series Engine 4+ line card when the interface is configured for shaping.

Workaround: Use a QoS group value in the range of one through seven in the policy map.

- CSCee93228

  Symptoms: Under certain unknown circumstances, a traceroute may trigger a process watchdog.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2. However, the problem is not specific to a Cisco 12000 series or to Cisco IOS Release 12.0S and may occur on other platforms and in Release 12.2T and Release 12.3.

  Workaround; There is no workaround.

- CSCee95978

  Symptoms: A Cisco router may reload unexpectedly with a Bus error exception.

  Conditions: This was observed on a Cisco 7200 series router with an NPE-G1 that was actively passing traffic.

  Workaround: There is no workaround.

- CSCef01537

  Symptoms: A VIP may reload because of a bus error when a corrupted FIBIDB is used unchecked by the router.

  Conditions: This symptom is observed rarely on a Cisco 7500 series when MQC is configured.

  Workaround Disable the MQC configuration.

- CSCef01689

  Symptoms: Transient errors may be generated when you boot a 1-port channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c, OC-12c/STM-4c) POS/SDH ISE line card. The errors disappear after some time.

  Conditions: This symptom is observed on a Cisco 12000 series when you boot the card line card by reloading either the router or the line card itself. The symptom occurs only when the peer router sends RIPv1 packets.

  Workaround: There is no workaround.

- CSCef03176

  Symptoms: A ping between two GRE interfaces may not work.

  Conditions: This symptom is observed when a GRE tunnel between two routers is up and you ping from the GRE interface of one router to the GRE interface of the other router.

  Workaround: There is no workaround.

- CSCef04202

  Symptoms: A QPPB-based service policy that is applied to an ATM interface may stop functioning, and traffic will no longer match the class map.

  Conditions: This symptom is observed when you reload a Cisco 10000 series that has QPPB configured on an ATM PVC.

  Workaround: There is no workaround.

- CSCef08388

  Symptoms: After a forced switchover, if you shut down a POS interface and save the configuration, the **shutdown** command does not show for this interface in the output of the **show running-config** command even though the output of the **show ip interface brief** shows that this interface is in the DOWN/DOWN state.

  Conditions: The symptom is observed on a Cisco 12410 and Cisco 12416 that run Cisco IOS Release 12.0(25)S4. The symptom does not occur for a Gigabit Ethernet interface.

  Workaround: There is no workaround.

- CSCef08774

  Symptoms: Certain types of fragmented packets are dropped when the ingress line card is an E6 line card and the egress line card is an E4+ line card. (CSCed22100 addresses this symptom for the E4+ line card.)

  Conditions: This symptom is observed on a Cisco 12000 series when there is an Engine 1 GE line card along the path before the traffic enters the E6 line card and when this Engine 1 GE line card does not have any features enabled.

  Workaround: Configure a feature such as Sampled NetFlow on the Engine 1 GE line card.

- CSCef09884

  Symptoms: The RP that is supposed to become the primary RP may crash when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(26)S3. This caveat is resolved in Release 12.0(26)S3.

  Workaround: There is no workaround.

- CSCef11214

  Symptoms: An Engine 2 Quad OC-12 POS line card release may fail when it is processing traffic.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(26)S3. This caveat is resolved in Release 12.0(26)S3.

  Workaround: There is no workaround.

- CSCef12828

  Symptoms: When traffic passes through a router, the router blocks traffic for certain prefixes behind a port-channel link. Traffic that originates from the router itself (that is, process-switched traffic) works fine.

  Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(27)S1 and that is configured with two PRP-2 processors.

  Workaround: There is no workaround.

- CSCef13024

  Symptoms: An Engine 2 line card in a Cisco 12000 series router does not forward packets destined to default route in hardware. Instead it is routed through the line card CPU.

  Conditions: Cisco IOS Release 12.0(27)S2 is affected by this problem.

  Workaround: There is no workaround. Traffic goes through the local CPU and so performance might be an issue.

  Further Problem Description: This problem is a side effect of the caveat CSCdz42137.

- CSCef14150

  Symptoms: The **show policy-map interface** command and its corresponding MIB, CISCO-CBQOS-MIB, report no or fewer Random Drops than what the router actually drops.

  Conditions: The problem occurs only on interfaces at or faster than 500 Mbps.

  Workaround: There is no workaround.

- CSCef16326

  Symptoms: When you remove a policy map from a subinterface, the subinterface may become stuck, preventing traffic from passing through the subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX7 when a nested policy map is applied to the main or physical interface in addition to the one that is already applied to the subinterface. The symptom could also occur in Release 12.0S.

  Workaround: Remove the policy map from the physical interface before you remove the policy map from the subinterface. When the subinterface configuration is updated, re-apply the policy map to the physical interface.

- CSCef23821

  Symptoms: Packet latency in a priority class is high when shaping is enabled in the parent class. For example, when you send 400 kbps of traffic through the priority class, the measured latency is about 80 ms.

  Conditions: This symptom is observed when the service policy has a shape average of 768000 on the class default and a child policy with a priority feature.

  Workaround: There is no workaround.

- CSCef24642

  Symptoms: The PXF engine on a Cisco 10720 may crash, and the following error messages are generated in the logging buffer (the PXF crashinfo files can be found in the flash memory of the router):

  ```
  MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
  ```

  In addition, there are four ways to verify that the symptom is occurring:

  – If the **debug main error**, **debug uplink error**, and **debug access error** commands are enabled on the router, the following error messages are also generated in logging buffer:

    ```
    MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error SRP_TX_VA_SC_GIANT_PKT
    (code 4)
    MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error
    SRP_TX_VA_SC_FIFO_GIANT_PKT(code 100)
    MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error
    VA_SC_IPM_RD_ACC_TIMER_EXP(code 1)
    MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error
    VA_RP_IPM_RD_ACC_TIMER_EXP(code 4)
    MSD: %Camr_VA-3-SISTATUS: Van Allen SRIC Data integrity error
    VA_SI_FL_CTRL_DRVN(code 80)
    MSD: %Camr_VA-3-SOSTATUS: Van Allen SROC Data integrity error VA_SO_PKT_LEN_ERR
    (code 1)
    ```

```
MSD: %Camr_VA-3-STATISTICS: VA statistics register: 0x0098 reports
VA_SO_PKT_LEN_ERR_COUNT =  3
```

- In the output of the **show interface srp 1/1** command, the received error counters such as "framer runts" and "input errors" have a large value.
- In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the "destination unreachable" counter increases.
- In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the "zero encap length" counter increases.

Conditions: This symptom is observed when all of the following conditions are present:

- A packet enters with or without an MPLS label.
- The router tries to send an ICMP packet to the source in any of the following situations:
  * The packet is denied by an output security ACL.
  * There is no route in the router to forward the packet.
  * The time to live (TTL) of the packet expires.
  * The packet is an ICMP echo request packet, and the router tries to send an ICMP echo reply packet to the source.
- On the interface on which the packet enters, the **ip unreachable** command is enabled by default.

Workaround: Enter the **no ip unreachable** command on all interfaces of the router, which works in the following two cases:

- The packet is denied by an output security ACL.
- There is no route in the router to forward the packet.

For other cases, there is no workaround.

- CSCef25866

  Symptoms: Connectivity for destinations that are reachable via an MPLS TE tunnel may fail when the tunnel is fast-rerouted. The loss of connectivity may result in loss of TCP sessions (BGP, LDP, etc.) for those destinations.

  When the problem happens, the output of the **show ip cef** *network* command shows "invalid cached adjacency" for the tunnel but does not show "fast tag rewrite."

  Conditions: This symptom is observed when all of the following conditions are present:

  - The adjacency of the primary tunnel becomes incomplete when FRR is active, as can be observed in the output of the **show adjacency** *type number* command. Whether or not the adjacency becomes incomplete is media-dependent. For example, with PPP the adjacency becomes incomplete but not with HDLC.
  - The primary tunnel is the only path to reach the prefix in question.
  - The **ip cef accounting non-recursive** command is not enabled.
  - A routing change occurs for the prefix after the FRR switchover. (This is topology dependent)

  Workaround:

  - Use HDLC encapsulation instead of PPP. This will prevent the adjacency from becoming incomplete.
  - Use forwarding adjacencies. This will prevent the routing change.

  Further Problem Description: The symptom affects traffic that originates on the tunnel headend. Transit traffic going through the tunnel is not affected. The symptom does not occur if there are multiple paths to the destination (one of which is the tunnel).

- CSCef25872

  Symptoms: An OC192E/POS-IR-SC line card in a Cisco 12000 series may crash with the following messages:

```
%GRP-4-RSTSLOT: Resetting the card in the slot: 4,Event: linecard error report
%MDX-1-DAEMSGSNDFAILED: FAILED to send IPC message of TYPE MDX_DAE_PULL_REQ to
slot 4 on the DAE,
        FAIL REASON = retry queue flush
%LCINFO-3-CRASH: Line card in slot 4 crashed
```

  Conditions: The symptom is seen when the ciscoOpticalMonitoringMIB is polled on a router running Cisco IOS Release 12.0(27)S1. The card that crashes does not have to be the card that is being polled. For example, an OC192E/POS-VSR in slot 0 may be polled with 1.3.6.1.4.1.9.10.83.1.1.1.1.8.2 and the OC192E/POS-IR-SC in slot 4 may crash.

  Workaround: Stop the crashes by configuring an SNMP view that prevents the ciscoOpticalMonitoringMIB from being polled.

- CSCef27191

  Symptoms: It is not possible to change the duplex configuration to full duplex on a Fast Ethernet (FE) interface of a Cisco 7200 series. When you enter the **full-duplex** interface configuration command, the command is ignored. The parser accepts the command, but it is not shown in the output of the **show running-config** command and the output of the **show interface** command shows the FE interface as half-duplex.

  Conditions: This symptom is observed when the FE interface belongs to a PA-2FEISL-FX or PA-2FEISL-TX port adapter and when the Cisco 7200 series runs Cisco IOS Release 12.0(28)S or a later release.

  Workaround: There is no workaround.

- CSCef27580

  Symptoms: Policy-based routing (PBR) loadsharing does not occur.

  Conditions: This symptom is observed on a Cisco 12000 series when PBR loadsharing is enabled via the **set next-hop recursive** command and when routes to the destination are available via multiple interfaces. When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that connects to the next-hop (or when the interface goes down and comes back up), traffic does not resume on this interface.

  Workaround: Enter the **static arp** command on the interface that connects to the next-hop.

- CSCef28848

  Symptoms: The following error message is generated repetitively for an ATM OC-12 line card:

```
%FIA-3-REQUESTERR: Request error was detected. Type = 1
```

  The output of the **show controller fia** command shows that the "Empty dst request" field continues to increment for the line card, and the line card is unable to pass multicast traffic.

  Conditions: This symptom is observed on a Cisco 12000 series when multicast packets do not have their Cisco cell fields properly set.

  Workaround: There is no workaround.

- CSCef31649

  Symptoms: A VRF interface receives auto-RP discovery packets only once via the core link. After that, no more RP discovery packets are received. After three minutes, the RP mapping table ages out, preventing multicast traffic from being passed.

Conditions: This symptom is observed on a Cisco 12000 series that has hardware-enabled multicast configured on a VRF interface.

Workaround: Disable hardware multicast on the VRF interface.

- CSCef31934

  Symptoms: In a scaled configuration with hundreds of eBGP peers with very low BGP timers, issuing **clear ip bgp *** may increase HW forwarding memory utilization.

  Conditions: This problem is seen with 500 eBGP sessions with BGP keepalive timer of 3 seconds and hold timer of 9 seconds. The router has 200K MPLS VPN routes. This problem is not seen if the BGP timers are set to the default value.

  Workaround: There is no workaround.

- CSCef40187

  Symptoms: An SRP interface is stuck and there is no response at all. In the output of the **show srp topology** command, the last topology packet that is received takes more than five seconds to arrive. In addition, the "zero encap length" counter in the output of the **show hardware pxf cpu stat interface srp 1/1 detail** command increases.

  Conditions: This symptom is observed on a Cisco 10720 when the value of the overall packet size divided by 32 is 1 or 2.

  Workaround: There is no workaround.

- CSCef41460

  Symptoms: Generic routing encapsulation (GRE) tunnel may not work on a provider edge (PE) router if VPN is configured.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(25)S or a later release.

  Workaround: There is no workaround.

- CSCef42706

  Symptoms: CPU hog, BGP sessions, and APS channels flaps are observed on routers.

  Conditions: When SNMP polling a Cisco 12000 series router with about 500 interfaces/subinterfaces, 900+ attached service policies, the router may produce CPUHOG log messages when polling the Class-Based-QoS-Mib stats.

  Workaround: There is no workaround.

- CSCef42815

  Symptoms: A flap of the BGP session between a primary provider edge (PE) router and a customer edge (CE) router that provides the default route may cause a remote CE router to lose Internet connectivity when the BGP session is restored.

  Conditions: This symptom is observed in a topology with CE routers that are dual-homed and connected to two Cisco 12000 series routers that function as PE routers and that run Cisco IOS Release 12.0(26)S2 when the default route is generated by a CE router in a different VPN routing/forwarding (VRF).

  Workaround: There are two steps to the workaround:

  1. Add a default VRF static route to cover the BGP-derived default route.
  2. Clear the default route entry in the routing table.

- CSCef42849

  Symptoms: Timing violation occurs in the PRE2/PRE1 temperature sensor routine. Since the temperature sensor routines violate timing requirements, the temperature reading fails in new device from a new vendor.

  Conditions: The failure occurs only in new temperature sensor from new vendor. All old type of sensors are not effected.

  Workaround: There is no workaround.

- CSCef44154

  Symptoms: When an MPLS packet that enters through an SRP or Ethernet interface contains an L2TP or UTI packet and this MPLS packet is processed by the RP instead of the PXF engine (for example, when the IP header in the MPLS packet contain options and the MPLS TTL equals 0 or 1), the SRP or Ethernet interface stops receiving packets.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

- CSCef44274

  Symptoms: The per-WRED-class drop counters are not incremented under **show queueing** output even though the aggregate WRED drops are non-zero.

  Conditions: The symptom is specific to the legacy random-detect command enabled under the main interface.

  Workaround: Attach a policy-map to the interface with random-detect enabled.

- CSCef48573

  Symptoms: An Engine 3 Quad OC-12 line card that is configured with multicast VPNs may punt traffic to the Route Processor (RP).

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(30)S. Note, however, that this caveat is resolved in Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCef52419

  Symptoms: In Cisco IOS software versions prior to Cisco IOS Release 12.0(27)S3, Release 12.0(28)S1, and Release 12.0(30)S, the Cisco 10720 router CPU utilization is high (x%/y%), where y is greater than 60%, and is reporting continuous BGP and LDP flapping. The **show interface** counters are showing a large number of drops and the **show buffers** command shows a large number of cache misses for the private IBC buffer pools.

  Conditions: The Cisco 10720 router is in a broadcast ARP storm environment and the interface **holdq <queue length> in** queue length is not the default of 75 packets for any one of the router's interfaces (for example, it is 2048).

  Workaround: Revert the **holdq <queue length> in** and **holdq <queue length> out** to the default setting by using the **default holdq in** and **default holdq out** commands on all interfaces with non-default hold queues.

- CSCef53085

  Symptoms: The rates that are specified in MQC wrongly include the L1 overhead. For example, if you configure the **bandwidth 100** command, 100 Kbps of L3 + L1 is guaranteed, excluding the L2 overhead. The throughput of L3 is therefore less than 100 kbps. (Note that the L2 overhead is not supposed to be included.)

Conditions: The symptom is observed in Cisco IOS Release 12.0(28)S and earlier releases.

Workaround: There is no workaround.

- CSCef53109

  Symptoms: A Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(8)S may experience following problem when the **do** command with arguments is issued from an interface member of a port-channel or pos-channel:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g 7/0/0
Router(config-if)#
Router(config-if)#do sh run int g 7/0/1
Command "do sh run int g 7/0/1" not allowed on link-bundle member interface
GigabitEthernet7/0/0
Router(config-if)#do sh ver
 Command "do sh ver" not allowed on link-bundle member interface
GigabitEthernet7/0/0
Router(config-if)#
```

  Conditions: The interface the command is issued from must be part of port-channel or pos-channel group.

  Workaround: Issue the command from the queried interface directly.

- CSCin24544

  Symptoms: A permanent virtual connection (PVC) configuration is removed if a PVC fails when it is recreated.

  Conditions: This symptom is observed on a Cisco 7500 series that has a Versatile Interface Processor (VIP). The PVC configuration may be removed if the VIP is carrying data traffic and the parameters of the virtual circuit (VC) class that is attached to the configured PVCs on the associated interface are modified.

  Workaround: There is no workaround.

- CSCin73658

  Symptoms: A Cisco 7500 series fails to handle IP packets with a size of 1499 or 1500 bytes if these packets are received over a PPP Multilink interface.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S when distributed multilink is configured.

  Workaround: There is no workaround.

- CSCin74347

  Symptoms: Outbound security ACLs are not applied properly on Cisco 10000 series routers.

  Conditions: This symptom is observed on all Cisco IOS Release 12.0 S images that contain the fix for CSCed72686.

  Workaround: There is no workaround.

- CSCin74920

  Symptoms: A spurious memory access may occur when a VC class with OAM parameters is created.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCuk51177

  Symptoms: You may not be able to make a Telnet connection to a Cisco IOS platform.

  Conditions: This symptom is observed when the CNS Exec Agent is used to remotely issue an interactive CLI command.

  Workaround: There is no workaround.

- CSCuk51269

  Symptoms: Multicast packets such as HSRP and OSPF are not received on a port-channel interface.

  Conditions: This symptom is observed when a port-channel interface is configured on a Cisco router, when you reload the router, and when the first member is added to the port-channel interface by entering the **no shutdown** interface configuration command on physical interface.

  Workaround: Enter the do **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port-channel interface.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Wide-Area Networking

- CSCdx84284

  Symptoms: A router may not recognize some inbound Multiprotocol Label Switching (MPLS)-tagged packets that are sent via Frame Relay. Because the router cannot recognize the inbound MPLS-tagged packets, MPLS cannot switch those packets to the outgoing interface. The MPLS-tagged packets are dropped by the router, and the router does not increment the input-packet counter in the output of the **show frame pvc** output EXEC command.

  Conditions: This symptom is observed on a Cisco router that has Cisco Express Forwarding (CEF) enabled and that is running Cisco IOS Release 12.2(7b). The symptom may also occur in other releases.

  Workaround: Enable the **debug mpls packets** EXEC command.

- CSCee62222

  Symptoms: The **frame-relay interface-dlci** command is removed unexpectedly from a point-to-point subinterface.

  Conditions: This symptom is observed when you enter the **clear frame-relay-inarp** command.

  Workaround: Do not use the **clear frame-relay-inarp** command.

- CSCee75882

  Symptoms: A GEIP+ that is installed in VIP may crash.

  Conditions: This symptom is observed on a Cisco 7500 series when the routing protocol adjacency of a neighbor is reset because an interface flaps.

  Workaround: Stabilize the routing protocol adjacency of the neighbor.

- CSCee85213

  Symptoms: A spurious memory access may occur and the following error message is generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x60C19208 reading 0x1C
  ```

  Under high-traffic conditions, the console freezes because of an alignment error.

  Conditions: These symptoms are observed on a Cisco 7200 series when a FR-FR local switched connection is configured by entering the **connect** command, when a queuing service policy is enabled on the main interface, and when the DLCI on the outgoing interface does not exist on the incoming interface.

  Workaround: Enter the **frame-relay route** command instead of the **connect** command. If the **connect** command is needed for access to features like policing, the errors do stop if the DLCI on the outgoing interface also exists on the incoming interface that has the service policy. The DLCI can be created under a subinterface that is shut down and that has no IP address configured if it is not used to handle traffic.

- CSCin74785

  Symptoms: A VIP crashes with the following error message:

  ```
  VIP-3-SYSTEM_EXCEPTION: VIP System Exception occurred sig=10, code=0x8
  ```

  Conditions: This symptom is observed when you remove a Frame Relay local switching connection from an MFR interface while traffic is running.

  Workaround: Shut down the connection or interface and ensure incoming traffic has stopped before you remove the connection.

- CSCuk51367

  Symptoms: A router may crash if a multipoint Frame Relay subinterface is deleted.

  Conditions: This symptom is observed only when there are multiple PVCs configured on the Frame Relay subinterface and when these PVCs have maps attached to the VCs.

  Workaround: Remove the individual maps and PVCs from the subinterface before you delete the subinterface.

Resolved Caveats—Cisco IOS Release 12.0(28)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(28)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdt26965

  Symptoms: A Cisco 7200 series router may generate %ALIGN-3-SPURIOUS alignment errors that may increase at a rate of one per second.

  Conditions: This symptom is observed when you reload the router and when a race conditions occurs. The occurrence of the symptom is unpredictable.

  Workaround: There is no workaround.

- CSCdz61503

  Symptoms: A Cisco router may reload when it performs Simple Network Management Protocol (SNMP) Notification Log MIB queries.

  Conditions: This symptom is observed on all versions of Cisco IOS software.

  Workaround: There is no workaround; however, the symptoms are not observed on a Cisco ONS 15530 or a Cisco ONS 15540 switch module because the symptoms have been resolved on these platforms.

- CSCeb20967

  Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an invalid memory address occurs while packets are placed into a hold queue.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S, 12.1(14)E4, or 12.2 S when the following sequence of events occurs:

  1. A packet is switched via Cisco Express Forwarding (CEF).
  2. The egress interface has queueing/shaping configured.
  3. The egress interface is congested, causing the packet to be placed into the hold queue.

  Workaround: There is no workaround.

- CSCeb49655

  Symptoms: A Cisco router may reload.

  Conditions: This symptom is observed on a Cisco router that is configured with distributed Cisco Express Forwarding (dCEF) and Cisco NetFlow and when the **deny** command in access-list configuration mode is configured on the subinterface of a Versatile Interface Processor (VIP).

  Workaround: Remove NetFlow or the access control list (ACL) from the subinterface.

Alternate Workaround: Do not use dCEF.

- CSCec22829

  Symptoms: A router may reload unexpectedly.

  Conditions: Same Timer wheel is used from both process level and interrupt level.

  Workaround: There is no workaround.

- CSCec39376

  Symptoms: A Flash memory card may become corrupted. The output of the **show** *flash-filesystem* EXEC command may display the following information:

  ```
  Open device slot0 failed (Bad device info block)
  ```

  Conditions: This symptom is observed on a Cisco platform when you perform an online insertion and removal (OIR) of the Flash memory card.

  Workaround: Do not perform an OIR of the Flash memory card. Rather, switch off the router and perform an offline insertion and removal.

  If the Flash memory card does become corrupted after an OIR, reformat the Flash memory card.

- CSCec70603

  Symptoms: You may not be able to specify authentication of a packet with encryption by using the **priv** keyword in the **snmp-server group** global configuration command.

  Conditions: This symptom is observed in Cisco IOS images that support 56- and 168-bit encryption.

  Workaround: There is no workaround.

- CSCec87661

  Symptoms: A "SYS-2-CHUNKBOUNDS" error message may be displayed on the router console. This message may be followed by a "NOTQ" error message.

  Conditions: This symptom is observed under rare circumstances during heavy usage of any application that is using chunks. The symptom is platform independent.

  Workaround: There is no workaround.

- CSCed00182

  Symptoms: A Cisco 7204VXR with an NPE400 may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco 7204VXR that runs the c7200-p-mz image of Cisco IOS Release 12.0(26)S.

  Workaround: There is no workaround.

- CSCed21186

  Symptoms: Incorrect "output IFMIB" counters are observed on the main interface.

  Conditions: This symptom has been observed on a Cisco 7500 series router running Cisco IOS Release 12.0(25)S1 when an 802.1q VLAN is configured with Committed Access Rate (CAR). The "output CLI" and "input SNMP/CLI" counters are correct.

  Workaround: There is no workaround.

- CSCed32794

  Symptoms: Executing the **tftp-server slaveslot0:** global configuration command, or any configuration commands related to tftp-server being set to access flash devices on the slave, will cause the slave to reload.

Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0(23)S5 but is not platform dependent.

Workaround: Configure the tftp-server to access flash devices on the master route switch processor (RSP) only.

- CSCed47820

  Symptoms: The Remote Processing Time reported by an SAA probe to a VRF/VPN loopback on a MPLS VPN PE router is too short, about 1~30ms, while the Round Trip Time that is calculated is too large, about >100ms. When you have probes sent to both an IPv4 Loopback and a VPNv4/VRF Loopback, you will see that the results they provide are exactly reverse to each other. For example:

```
router time type    remote process time    roundtrip delay
saa_probe2ipv4                      218                  1
saa_probe2vpnv4                       5                219
```

  Conditions: This symptom is observed when an SAA probe is sent to VPN/VRF addresses on an MPLS VPN PE router through a MPLS VPN network.

  Workaround: There is no workaround.

- CSCed54444

  Symptoms: A Cisco 10000 series functioning as a LAC may become very busy and start queueing up the incoming L2TP packets from an LNS, causes the middle buffer to become exhausted and eventually use all available IO memory. Malloc failures with tracebacks can be seen in the log.

  Conditions: This symptom is observed when disconnecting L2TP sessions at 200 calls per second or more.

  Workaround: There is no workaround.

- CSCed77666

  Symptoms: SAA RTR key-chain authentication may fail with the following RTT responder:

  authentication failure

  Conditions: This symptom is observed when SAA is using a key chain which has a key ID that has a value larger than 255.

  Workaround: Ensure that the value of the key ID does not exceed 255.

- CSCin72727

  Symptom 1: The ifOperStatus SNMP object may return “Testing” when the CLI states Up/Up (Looped).

  Condition 1: This symptom is observed when PPP encapsulation and loopback are configured.

  Workaround 1: There is no workaround.

  Symptom 2: The ifOperStatus SNMP object may return “DOWN.”

  Condition 2: This symptom is observed when HDLC encapsulation and the **down-when-looped** command are configured.

  Workaround 2: There is no workaround.

Interfaces and Bridging

- CSCdv57198

  Symptoms: A Cisco router may forward the MAC-layer broadcast.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1(10) but may also occur in other releases.

Workaround: There is no workaround.

- CSCea62753

  Symptoms: Fragments produced on a Route Switch Processor (RSP) may be corrupted. The fragments may have extra bytes of garbage that may cause the remote end to drop the packets since the remote end cannot rebuild the packets.

  Conditions: This symptom occurs on a Cisco 7500 router that is configured for Frame Relay fragmentation 12 (FRF.12) on a Packet-over-SONET (POS) subinterface.

  Workaround: There is no workaround.

- CSCec87736

  Symptoms: TX Simple Network Management Protocol (SNMP) counters do not update on Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic.

  Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S and Release 12.3. The hardware is DEC21140A, and the interface receiving the traffic is not located on the same Versatile Interface Processor (VIP).

  Workaround: There is no workaround.

- CSCed08399

  Symptoms: A Cisco 7500 series may generate spurious memory accesses at a VIP.

  Conditions: This symptom is observed when CRTP is enabled on the interfaces of the VIP.

  Workaround: There is no workaround.

- CSCed29590

  Symptoms: An interface on a Cisco 7500 series that is configured for distributed Multilink PPP (dMLP) may stop transmitting data.

  Conditions: This symptom is observed when the links in an MLP bundle flap. When the router detects that the interface does not transmit data, the router automatically resets all Versatile Interface Processors (VIPs) to restore proper functioning.

  The following log information shows the sequence of events when the symptom occurs:

```
%LINK-3-UPDOWN: Interface Serial10/1/1/11:23, changed state to down
%LINK-3-UPDOWN: Interface Serial10/1/1/12:23, changed state to down
%LINK-3-UPDOWN: Interface Multilink9, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/1/1/11:23, changed
                     state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/1/1/12:23, changed
                     state to down
%LINK-3-UPDOWN: Line protocol on Interface Multilink9, changed
%LINK-3-UPDOWN: Interface Serial10/1/1/12:23, changed state to up
%LINK-3-UPDOWN: Interface Multilink9, changed state to up
%LINK-3-UPDOWN: Interface Serial10/1/1/11:23, changed state to up
%RSP-3-RESTART: interface Serial10/1/1/11:23, output frozen
%RSP-3-RESTART: cbux complex
```

  Workaround: There is no workaround.

- CSCed47550

  Symptoms: BGP Policy Accounting information is not available via SNMP for 802.1Q VLAN subinterfaces.

  Conditions: This symptom is observed on Cisco 12000 and 7500 series routers.

  Workaround: There is no workaround.

- CSCin64671

  Symptoms: A Cisco RSP VIP can crash during bootup.

  Conditions: This symptom is observed on a Cisco 7500 series when the Cisco IOS software image is booted.

  Workaround: There is no workaround.

- CSCuk47970

  Symptoms: The "PARSER-3-BADSUBCMD" error message is frequently observed when you enter the **media-type 100baset** command on Fast Ethernet interfaces.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdv57965

  Symptoms: Although you may able to configure more than 4 Gbps of bandwidth for Resource Reservation Protocol (RSVP) or for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, the actual reserved bandwidth that is established for RSVP or the MPLS TE tunnel may be much less than 4 Gbps.

  The output of the **show running-config interface** *type number* privileged EXEC command shows the configured bandwidth. The output of the **show ip rsvp reservation** EXEC command shows the actual reserved bandwidth for RSVP.

  Conditions: This symptom is observed when the interface on which RSVP or the MPLS TE tunnel is configured does have sufficient bandwidth available to satisfy the configured bandwidth but the actual reserved bandwidth is less than the configured bandwidth.

  Workaround: There is no workaround.

- CSCeb19857

  Symptoms: A Cisco router may pause indefinitely on reload with a traceback and bus error exception.

  Conditions: This symptom may be observed with a Cisco Open Shortest Path First (OSPF) router that is doing redistribution.

  Workaround: There is no workaround.

- CSCeb57553

  Symptoms: A router may crash when you enter the **no vpdn** command to clear a tunnel and then you enter any command that requires intensive CPU utilization (for example, a command that clears a large number of static routes).

  Conditions: This symptom is observed when a high number of PPPoE session is configured.

  Workaround: Avoid commands that require intensive CPU utilization while clearing the sessions.

- CSCec07592

  Symptoms: The best path is not chosen correctly on a Cisco router.

  Conditions: This symptom is observed when the **bgp deterministic med** router configuration command is configured on a Cisco router. The symptom occurs when different values of Multi Exit Discriminator (MED) are set for peers. In this particular situation, the symptom occurs when different values of MED are set to different peers.

  Workaround: There is no workaround.

- CSCec07636

  Symptoms: When the following Open Shortest Path First (OSPF) MIB tables are queried via snmpwalk, some interfaces may not be displayed:

  – ospfNbrTable
  – ospfIfTable
  – ospfIfMetricTable

  Conditions: This symptom is observed on any Cisco platform that runs OSPF.

  Workaround: There is no workaround.

- CSCec23167

  Symptoms: During BGP scalability testing, error messages and tracebacks similar to the following ones may be logged, indicating a difficulty with TCP and buffer usage:

```
%SYS-2-MALLOCFAIL: Memory allocation of 4692 bytes failed from 0x6076F714,
align
Pool: I/O  Free: 11143248  Cause: Memory fragmentation
Alternate Pool: None  Free: 0  Cause: No Alternate pool
-Process= "Pool Manager", ipl= 0, pid= 6
-Traceback= 607FE10C 607FF1EC 6076F71C 6080C1D0 6080C400
%TCP-6-NOBUFF: TTY0, no buffer available
-Process= "BGP I/O", ipl= 0, pid= 139
-Traceback= 6098B4EC 609938C8 60993C1C 60D55CE4 60D0BEB0
%TCP-6-NOBUFF: TTY0, no buffer available
-Process= "BGP Router", ipl= 0, pid= 138
-Traceback= 6098B4EC 609938C8 60993C1C 60D55CE4 60D29858 60D2AF88 60D1B4BC
```

  Conditions: This symptom is observed on a Cisco router that is in the processing of building BGP sessions for about 80,000 prefixes and about 1200 BGP peers.

  Workaround: There is no workaround.

- CSCec55418

  Symptoms: A Cisco router may reload unexpectedly at “ospf_area_delete().”

  Conditions: This symptom is observed on a router that is configured for Open Shortest Path First (OSPF) when all of the following conditions are present:

  – A large number of **network** commands are removed from the configuration at once via a cut-and-paste operation.
  – All of the **network** commands for an area are removed.
  – A **no area** command is entered for an area that is referenced in the **network** commands.

Workaround: Do not use a cut-and-paste operation to remove the **network** commands simultaneously with the area that is referenced in the **network** commands.

- CSCec70366

  Symptoms: When the multicast route (mroute) expiration timer is set to a nondefault holdtime value, a router may reload unexpectedly because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco router when a nondefault holdtime value is received via a Protocol Independent Multicast (PIM) join message in combination with a bursty source. This situation may cause the mroute expiration timer to enter an infinite loop.

  Because the holdtime value is not user configurable on a Cisco router, this situation is caused by a PIM connection with a non-Cisco router or by the modification of the Internet Group Management Protocol (IGMP) query interval on an interface.

  Workaround: Ensure that no nondefault holdtime value can be configured for PIM or IGMP.

- CSCec70428

  Symptoms: When Protocol Independent Multicast (PIM) dense mode is enabled, an interface in the outgoing interface list may indicate that it is in forwarding mode but the P flag may still be set to the source, group (S,G) state, preventing the interface from forwarding any packets.

  Conditions: This symptom is observed when an interface enters the forwarding mode because the prune timer expires and when there is an Internet Group Management Protocol (IGMP) member on this interface.

  Workaround: Enter the **clear ip mroute** *group* privileged EXEC command.

- CSCec85322

  Symptoms: A Cisco router may reload unexpectedly while running Open Shortest Path First version 3 (OSPFv3) in a negative testing environment.

  Conditions: The symptom is observed under rare circumstances when the router is running low on memory and when a successful memory allocation (MALLOC) occurs just before the router reloads.

  Workaround: There is no workaround.

- CSCec90041

  Symptoms: BGP update generation may enter a deadlock.

  Conditions: This symptom is observed when the RR configuration is changed.

  Workaround: Remove the BGP process and add it back.

- CSCed00449

  Symptoms: SAA probes that are executing on the Cisco 12000 series routers incorrectly measure round trip time delay measurements.

  Conditions: This symptom is only observed on a Cisco 12000 series router.

  Workaround: Run the probe on a different Cisco platform.

- CSCed19765

  Symptoms: On a router with the **ip routing external overload signalling** hidden command enabled, if a router-wide CEF FIB-DISABLE event takes place (rather than a FIB-DISABLE event on a line card), the loopback interface and its associated IP address are removed from the routing table.

  On FIB recovery, the IP address associated with the loopback interface will not be present in the routing table and therefore cannot be advertised to any other routers in the network.

Conditions: This behavior is observed in Cisco IOS Release 12.0(25)S and later releases on a router with the **ip routing external overload signalling** hidden command enabled. Earlier Cisco IOS releases are not affected.

Workaround: Enter the **no ip routing external overload signalling** hidden command.

- CSCed26217

  Symptoms: Even if an OSPF neighbor is in the "FULL" state and an ARP entry exists, a Cisco platform still sends (and receives) ARP requests at an interval specified in the "poll-interval."

  Conditions: This symptom is observed on a Cisco platform with dual RPs when you configure an interface as an OSPF nonbroadcast network interface and set the "poll-interval" for a neighbor that is part of the nonbroadcast segment.

  Workaround: There is no workaround.

- CSCed35907

  Symptoms: When the following CLI sequence is configured, the router may run into a race condition and crashes:

  router ospf 100

  router ospf 1000 vrf *vrf-name*

  then

  no router ospf 100

  router ospf 1000

  no router ospf 1000

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.3(4)T and later releases. A configuration script with the above CLI sequence is run on the router. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed41323

  Symptoms: A Cisco router with a label switched path (LSP) tunnel on which Fast ReRoute (FRR) is enabled and active may stop refreshing the Resource Reservation Protocol (RSVP) state when the refresh updates are received via RSVP summary refresh messages. This situation causes the RSVP to time out and the LSP tunnel to be torn down.

  Conditions: This symptom is observed on a Cisco router that does not transmit RSVP messages for LSP tunnels on which FRR is enabled and active via message IDs. The symptom does not occur when FRR is enabled but not active.

  A peer router that runs software other than Cisco IOS software may continue to send RSVP messages with messages IDs that request an acknowledgment. The Cisco router does acknowledge these message IDs, causing the peer router to start sending RSVP summary refresh messages to refresh the RSVP state. The Cisco router ignores the message IDs that are contained in these RSVP summary refresh messages and does not refresh the RSVP state.

  Workaround: There is no workaround.

- CSCed53358

  Symptoms: Pings fail on an Ethernet-to-VLAN interworking over L2TPv3 due to an IRDP failure.

  Conditions: This symptom is observed when you ping between two CE routers. Both of the CE routers do not learn each other's MAC address automatically.

  Workaround: Ping from the first CE router to the second CE router, then ping from the second CE router to the first CE router.

- CSCed55567

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed after you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command multiple times on different interfaces.

  Workaround: There is no workaround.

- CSCed60289

  Symptoms: IP background process is sluggish.

  Conditions: This symptom occurs when many interfaces go down at the same time.

  Workaround: There is no workaround.

- CSCed60800

  Symptoms: The withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table.

  Conditions: This symptom is observed when the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured.

  Workaround: Enter the **clear ip bgp *** or disable the **maximum-paths eibgp** command or **maximum-paths ibgp** command.

- CSCed62633

  Symptoms: A router may crash after the IP address of the interface of a neighboring router is changed while an MPLS TE tunnel is using this interface.

  Conditions: This symptom is observed on a Cisco router that functions as a midpoint of an MPLS traffic engineering (TE) tunnel and occurs shortly after the IP address of the ingress interface of the downstream neighboring router is changed while the MPLS TE tunnel is using this interface.

  Workaround: There is no workaround.

- CSCed62901

  Symptoms: This symptom occurs in an OSPF network topology in which a CE router (CE-1) connect to a PE router (PE-1) that connects to two other PE routers (PE- 2 and PE-3), each of which connect to another CE router (CE-2 and CE-3). In turn, both of these CE routers are connected to each other (that is, CE-2 and CE-3 connect to each other).

  When the link between the PE-3 and the CE-3 flaps, the OSPF route in the VRF fails to switch back from BGP to OSPF on the PE-1.

  Conditions: This symptom is observed in Cisco IOS Release 12.0 S, 12.2 S, and 12.3 T.

  Workaround: Clear the ip route, clear the OSPF process, or enter the **clear ip bgp *** command on the PE-1 to bring the route back from BGP to OSPF.

- CSCed70979

  Symptoms: A router may reload unexpectedly with a bus error and/or display spurious memory access messages.

  Conditions: This symptom is observed when the router is configured for OSPF and is actively learning OSPF routes dynamically.

  Workaround: There is no workaround.

- CSCed75295

  Symptoms: FRR LSPs may fail to provide protection with a Next-next-hop (NNHOP) backup tunnel.

  Conditions: This symptom is observed only when a primary LSP reaches beyond a merge point.

  Workaround: There is no workaround.

- CSCed82273

  Symptoms: IPv6 BGP may not reach the established state.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(26)S2 or Release 12.0(28)S. However, the symptom is not platform-specific.

  Workaround: There is no workaround.

- CSCee10426

  Symptoms: A BGP prefix may receive or advertise incorrect label information.

  Conditions: This symptom is observed on an MPeBGP session between ASBRs when there is more than one MPeBGP session configured.

  Workaround: There is no workaround.

ISO CLNS

- CSCec39973

  Symptoms: A router that runs Intermediate System-to-Intermediate System (IS- IS) may reload unexpectedly when there are a lot of adjacencies that continue to flap.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2 S.

  In Release 12.0 S, the symptom may occur when you enter the **router isis** global configuration command followed by the **fast- flood** router configuration command.

  In Release 12.3, the symptom may occur when you enter the **router isis** global configuration command followed by the **ip fast- convergence** router configuration command.

  Workarounds: Prevent IS-IS adjacencies from flapping. There is no other workaround for Release 12.2 S.

  For Release 12.0 S, do not enter the **router isis** global configuration command followed by the **fast-flood** router configuration command.

  For Release 12.3, do not enter the **router isis** global configuration command followed by the **ip fast-convergence** router configuration command.

- CSCed40888

  Symptoms: A Border Gateway Protocol (BGP) session may be terminated unexpectedly.

  Conditions: This symptom is observed on a Cisco router that functions as a peer in a BGP configuration when you disable and reenter the **neighbor** *ip-address* **send-label** address family configuration or router configuration command or when you move the router that has the **neighbor** *ip-address* **send-label** address family configuration or router configuration command enabled to a peer group.

  Workaround: There is no workaround.

Miscellaneous

- CSCdx83013

  Symptoms: A Cisco 7200 series router may reload when you insert an ISDN BRI port adapter.

  Conditions: This symptom is observed on Cisco 7200 series router that is configured with a Network Processing Engine G1 (NPE-G1).

  Workaround: There is no workaround.

- CSCdy40928

  Symptoms: Connectivity difficulties may occur when Virtual Private Network (VPN) routing/forwarding (VRF) packets follow the global routing table instead of the VRF table.

  Conditions: This symptom is observed on a low-end Cisco router that runs Cisco IOS Release 12.2(7a) or another release when the global address space in the router overlaps with the VRF address that is configured on a VRF interface of a connected PE router. The VRF interface of this PE router may be unreachable but end-to-end connectivity may not be affected.

  Workaround: There is no workaround.

- CSCdy51250

  Symptoms: Incoming packets may be lost or may pause indefinitely on the native Gigabit Ethernet interfaces of a Network Processing Engine G1 (NPE-G1) that is installed in a Cisco 7200 series router.

  Conditions: This symptom is observed under a full traffic load and only on a Cisco 7200 series router that is configured with an NPE-G1. Other NPEs work fine.

  Workaround: There is no workaround.

- CSCdz63050

  Symptoms: Outdrops may occur on a native Gigabit Ethernet interface of a Network Processing Engine G1 (NPE-G1), and the "bad length" counter in the output of the **show controllers gigabitethernet** privileged EXEC command may increase.

  This situation may prevent a customer premises equipment (CPE) from using FTP and HTTP communication when the CPE is connected to the Internet via a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) and a L2TP network server (LNS).

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1, that is functioning as an LNS, and that has Cisco Express Forwarding (CEF) enabled.

  Workaround: Enter the **no ip cef** global configuration command.

- CSCea60917

  Symptoms: When a Cisco 10000 series configuration includes excessive numbers of PBR route-map policies or excessive numbers of route-maps (that is, sequence numbers) in any PBR route-map policy, the excess route-map policies and/or route-maps per policy may be ignored (which is correct behavior), and an error message and traceback message similar to the following may be displayed:

  ```
  %GENERAL-3-EREVENT: too many C10K PBR policy maps
  -Traceback= 60BBB63C 60BBC784 605E1F14 6032363C 60334274 60334524 603345C4 603F4
  ```

  Conditions: This symptom is observed when more than 256 PBR route-map policies are configured or when more than 32 route-maps (that is, sequence numbers) are configured in any PBR route-map policy.

The display of a traceback message is too severe in this situation. The correct behavior is that the excess route-map policies and/or route-maps per policy should be ignored, and an informational message should be displayed. This informational message should state that the Cisco 10000 series PBR limits for route-map policies and/or route-maps per policy has been exceeded.

Workaround: Ensure that the PBR configurations on a Cisco 10000 series limits do not exceed 256 PBR route-map policies or 32 route-maps per policy.

- CSCea63499

  Symptoms: A Cisco 7200 may reload unexpectedly when it attempts to translate virtual address 0x3C0C00C0 to a physical address.

  Conditions: This symptom is observed under rare conditions on a Cisco 7200 that is configured with a C7200-I/O-FE I/O controller in slot 0. The symptom is related to an error in the Fast Ethernet controller on the I/O controller.

  Workaround: There is no workaround.

- CSCeb21815

  Symptoms: The serial interface of a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may remain down.

  Conditions: This symptom is observed on a PA-MC-STM-1 that is installed in a Cisco 7600 series when an internal resource allocation does not occur. The symptom may also occur on other platforms in which a PA-MC-STM-1 is installed.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCeb45929

  Symptoms: An Enterprise Systems Connection (ESCON) Channel Port Adapter (ECPA), Parallel Channel Port Adapter (PCPA), or ECPA version 4 (ECPA4) fails to reactivate after a microcode reload or an online insertion and removal (OIR) and displays the following messages:

  ```
  Router# microcode reload ecpa4 slot 4
  Reload microcode? [confirm]
  %PA-4-IMPROPER_REMOVAL: Improper removal for slot 2.
  %PA-3-DEACTIVATED: port adapter in bay [2] powered off.
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that has an ECPA, PCPA, or ECPA4 configured.

  Workaround: Reload the router.

- CSCeb68673

  Symptoms: On an ASBR-PE, the TFIB may be missing a forwarding entry for a prefix that is learnt from a PE.

  Conditions: This symptom is observed on an “ABSR-co-located PE” (that is, an ASBR that also functions as a PE router) when the PE functionality is removed by deconfiguring VRF, for example, by entering the **no ip vrf** *vrf-name* command.

  Since this is a timing issue, it may occur in Cisco IOS Release 12.0 S, 12.2 S, 12.2 T, and 12.3.

  Workaround: There is no workaround.

- CSCeb70755

  Symptoms: Sporadic error recovery may occur on an Engine 4 plus (E4+) line cards after a corrupt packet that comes from the fabric is detected. The error recovery is indicated by %TX192-3-PAM_MODULE and %TX192-3-PAM_PIM error messages on the E4+ line card. The packets are corrupted by Engine 3 line cards and are triggered by routing convergence.

  Conditions: This symptom is observed on a Cisco 12416 router that runs Cisco IOS Release 12.0(25)S or Release 12.0(25)S1. Only packets in the IP-to-tag path are affected.

  Workaround: There is no workaround.

- CSCeb73894

  Symptoms: You may not be able to load a Cisco IOS software image onto a Cisco 12000 series from an Advanced Technology Attachment (ATA) Flash disk, and one or more error messages similar to the following may appear:

  ```
  open(): Open Error = -13 loadprog: error - on file open boot: cannot load
  "disk0:gsr-p-mz.120-24.S2"
  ```

  ```
  open: read error...requested 0x4 bytes, got 0xffffffff trouble reading device magic
  number loadprog: error - on file open boot: cannot load "disk0:gsr-p-mz.120-22.S3c"
  ```

  Conditions: This symptom is observed when the ATA disk is formatted with one Cisco IOS software image and also contains another Cisco IOS software image that you attempt to load onto the Cisco 12000 series.

  Workaround: Enter the **boot system tftp** *filename ip-address* global configuration command, **dummy** for the *filename* argument, and **10.1.1.1** for the *ip-address* argument. Note that this command parses without errors, and then fails; the router may not appear to boot initially, but eventually does so.

  Further Problem Description: The symptom only affects a Cisco 12000 series RP. It does not affect a Cisco 12000 series PRP.

- CSCeb87765

  Symptoms: A line card may crash when a class is removed from a policy map and this policy map is attached to two different interfaces that are configured as IPv6 interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series when the removed class is configured for both WRED and traffic shaping.

  Workaround: Do not attach the same service policy to two different IPv6 interfaces.

- CSCec07354

  Symptoms: On dual Performance Route Processors (PRPs) in RPR+ mode, the secondary PRP may not boot up. When you log into the PRP, it appears to be in the ROMmon state.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S1 when the ROM monitor of the primary RPR is upgraded.

  Workaround: Attach to the secondary RPR and boot up this RPR manually by entering the **boot** command on the ROMmon prompt.

- CSCec08364

  Symptoms: Ethernet over Multiprotocol Label Switching (EoMPLS) packet forwarding may stop.

  Conditions: This symptom is observed when you configure an IP address on the EoMPLS interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the EoMPLS interface.

- CSCec14039

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed on a Cisco 7200VXR series that is configured with an NPE-G1 Network Processing Engine

  Workaround: There is no workaround.

- CSCec18507

  Symptoms: A label controlled ATM (LC-ATM) interface may have extra LVCs for one prefix; the output of the **show mpls atm-ldp bindings** *network mask* privileged EXEC command displays two destination entries for the same prefix. For one of these destination entries, all LVCs are in the active state. For the other destination entry, all LVCs are in bindwait state.

  Data forwarding to the destination does go through the active LVCs and works fine.

  Conditions: This symptom is observed when Multi-VC mode enabled on the LC-ATM interface and when quick route flapping occurs for a while.

  Workaround: Enter the **clear ip route** *network mask* EXEC command.

- CSCec22929

  Symptoms: A software-forced reload may occur on a Cisco 7200 series after an OIR of a PA-2T3+ port adaptor.

  Conditions: This symptom is observed when traffic enters through the interface of the port adapter.

  Workaround: Shut down the interface of the port adapter before you perform an OIR.

- CSCec33028

  Symptoms: A 1-port E3 serial port adapter (PA-E3) may fail to recover to the “up/up” state even when the original cause of the failure is corrected.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the PA-E3.

- CSCec36978

  Symptoms: A Cisco 7500 series that is configured with a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may reload unexpectedly.

  Conditions: This symptom is observed when the following steps occur in sequence:

  1. You enter the **shutdown** controller configuration command on the controller of the PA-MC-STM-1.

  2. You enter the **write memory** EXEC command.

  3. You reload the router.

  4. You enter the **no shutdown** controller configuration command on the controller of the PA-MC-STM-1.

  Workaround: There is no workaround.

- CSCec45307

  Symptoms: There may be no memory for the expanded TFIB PSA. The label allocation may fail with error messages that are shown below and may be followed by a memory traceback.

  ```
  %TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag
  ```

```
%TFIB-2-MEMORY: No memory for expanded TFIB PSA
-Traceback=
```

Conditions: This symptom is only observed on an MPLS-capable Cisco platform and only when the label space has been exhausted to the maximum level supported by the platform or is about to be exhausted (only a few hundred labels are available) and when the TFIB table is expanded further.

Workaround: Enter the **mpls label range 16 101900** command at the conf-t level to avoid the error messages.

- CSCec46191

  Symptoms: When you securely copy a Cisco IOS image to a flash disk by entering the **copy scp slot0:** or **copy scp slot1:** EXEC command, the copy process may stop after about 60 to 70 percent has been transferred.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(25)S1 or Release 12.3.

  Workaround: Copy the Cisco IOS image via another transport protocols such as TFTP.

- CSCec48428

  Symptoms: “OSPF-4-ERRRCV” and “OSPF-4-BADLENGTH” error messages are observed, and a ping of the directly connected interface may experience 20 percent failure.

  Conditions: These symptoms are observed when connecting an IP Services Engine (ISE) OC-48 line card to the router of another vendor at the far end. It is observed that after reloading the other router that the ISE OC-48 line card could be stuck in a bad state, which may cause corrupted packets.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ISE OC-48 interface.

- CSCec55147

  Symptoms: A small memory leak is experienced on a Cisco router.

  Conditions: The problem appears only in the corner case when ftp operation aborts in the middle and results in a few bytes of memory leak. The memory leak does not happen otherwise. This does not impact any other router operation.

  Workaround: There is no workaround.

- CSCec57763

  Symptoms: A VIP may reload when an SSO occurs on an RP.

  Conditions: This problem occurs intermittently when distributed MLP is configured on the router.

  Workaround: There is no workaround.

- CSCec63687

  Symptoms: An E3 4xOC12 channelized line card keeps resetting.

  Conditions: This symptom is observed under load sharing between a POS channel interface and a regular POS interface.

  Workaround: There is no workaround.

- CSCec63942

  Symptoms: With a PRP running Cisco IOS Release 12.0(25)S1, the PRP hangs after the **test crash** command is entered. This is seen only on a PRP-1 and not a GRP-B.

Conditions: These symptoms are observed on a Cisco 12000 router with a PRP-1 and a full or nearly full chassis after the **test crash** command is entered. The router becomes inaccessible and inoperable. This only happens when the **exception warmstart 60 5** global configuration command is configured.

Workaround: Disable the **exception warmstart** global configuration command. Note, however, that when you do so, caveat CSCeb70797 may occur.

- CSCec64576

  Symptoms: An 8XOC3 ATM line card stops passing non-exp0 traffic (that is, tagged packets with the exp field in the MPLS shim not equal to zero) after an RP or line card reloads.

  Conditions: This problem happens when ingress and egress subinterfaces are configured on the same ATM interface using an ATM switch. This symptom is observed on Cisco IOS Release 12.0(25)S3 or a later release.

  Workaround: To recover the interface, enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCec69091

  Symptoms: When an ATA disk is formatted on a router that shares ATA-Monlib within its CPU family, any disk-related CLIs may log the following information:

  ```
  PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a different router or PC. A format
  in this router is required before an image can be booted from this device
  ```

  Conditions: This symptom is observed on a Cisco router that shares ATA-Monlib within its CPU family such as a Cisco 6400 series NSP and a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCec70350

  Symptoms: An E3 card crashes when more than 10k multicast groups are created, and traffic is sent to these groups. This is seen with sparse mode and Auto- RP.

  Steps for crash:

  1. Advertise 130k BGP routes.

  1a. Send traffic to port advertising the BGP routes.

  2. Advertise 10000 multicast groups. (When tried with 300 groups, card did not crash.)

  3. Send traffic to multicast groups.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: Do not create 10k multicast groups.

- CSCec73063

  Symptoms: An output wedge and drops may occur on the multilink interface of a Cisco 7200 series. The output of the **show interfaces** privileged EXEC command may display the following information:

  ```
  .
  .
  .
  Multilink3 is up, line protocol is up
  .
  .
  .
  ```

```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 5526
  Queueing strategy: fifo
  Output queue: 31/40 (size/max)
.
.
.
```

Conditions: This symptom is observed on a multilink interface that has two E1 interfaces in a multilink bundle when there is a low traffic rate.

Workaround: Use the physical interface without a multilink bundle.

- CSCec77256

  Symptoms: Basic VPN with SRP Dense (E4P) links fail the ping test.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running the Cisco IOS Release 12.0 S image gsr-p-mz.

  Workaround: There is no workaround.

- CSCec77478

  Symptoms: When a Cisco IOS software image runs on a standby Performance Routing Engine (PRE) together with an older version of Cisco IOS software that runs on the primary PRE, the following error message may appear on the standby router:

  ```
  %IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP: Cannot find IDB index table entry: "", 79
  ```

  After a switchover from the primary PRE to the standby PRE occurs, the interfaces for which the above error messages appear may not be able to send or receive packets.

  Conditions: This symptom is observed on a Cisco 10000 series during a Fast Software Upgrade (FSU) operation.

  Workaround: There is no workaround.

- CSCec78439

  Symptoms: MQC service policies applied to either Multilink PPP or FR interfaces cannot be viewed operationally after an RP switchover.

  Conditions: This condition is observed for service policies applied to multilink interfaces and occurs after a Cisco 12000 series router with either dual GRPs or PRPs that are running either SSO or RPR+ redundancy mode executes a switchover.

  Workaround: There is no workaround.

- CSCec78545

  Symptoms: A Versatile Interface Processor (VIP) may reload when the **clear cef line** command is entered or when a new VRF is provisioned on an interface via the CLI.

  Conditions: This symptom is observed on a VIP when Multiprotocol Label Switching (MPLS), Egress NetFlow, and distributed Cisco Express Forwarding (dCEF) are configured.

  Workaround: Disable dCEF or Egress NetFlow before making configuration changes or before entering the **clear cef line** command.

- CSCec79849

  Symptoms: A line card may experience high CPU usage, and report alignment and spurious memory access error messages.

  Conditions: This symptom is observed on the line card of a Cisco 12000 series Internet router.

  Workaround: There is no workaround.

- CSCec80283

  Symptoms: An IP Services Engine (ISE) line card may display high CPU utilization.

  Conditions: This symptom is observed on an ISE line card in a Cisco 12000 series when Multiprotocol Label Switching (MPLS) packets are sent to the nonlabel-switched interface of the ISE line card.

  Workaround: There is no workaround.

- CSCec80703

  Symptoms: Tracebacks may occur when you configure or deconfigure automatic protection switching (APS) on a 4-port OC-3 ATM line card.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround. Note that the functionality of the line card and router is not impaired.

- CSCec82298

  Symptoms: A software-forced reload may occur on a Cisco 12000 series router.

  Conditions: This symptom is observed on a Cisco 12000 series router after a service policy is enabled.

  Workaround: There is no workaround.

- CSCec86102

  Symptoms: Tag entries may be missing on a Versatile Interface Processor (VIP).

  Conditions: This symptom is observed on a Cisco 7500 series that has distributed Cisco Express Forwarding (dCEF) enabled.

  Workaround: Enter the **clear cef linecard** user EXEC or privileged EXEC command.

- CSCec86131

  Symptoms: A FlexWAN or VIP in which a channelized port adaptor such as a PA-STM1 or PA-MC-8TE1+ is installed may reload continuously.

  Conditions: This issue is seen when distributed LFI is configured on channelized serial interfaces and heavy traffic (close to line rate) occurs on these interfaces.

  Workaround: There is no workaround.

- CSCec88027

  Symptoms: An Engine 4 Plus (E4+) Gigabit Ethernet (GE) or Fast Ethernet (FE) line card that is configured with Any Transport over MPLS (AToM) may fail.

  Conditions: This symptom is observed on an E4+ GE or FE line card on a Cisco 12000 series router that is running Cisco IOS Release 12.0(26)S as soon as a soft online insertion and removal (OIR) is performed on the primary clock scheduler card (CSC).

  Workaround: There is no workaround.

- CSCed00033

  Symptoms: When an ATM PVC bounces, it fails to come back up and remains in the DOWN/UNVERIFIED state.

  Conditions: This symptom occurs when an ATM LC is connected to an ATM switch. Also, the ATM PVC is managed by OAM, and the frequency of the OAM F5 loopback cells is set to 0, via the **oam-pvc manage 0** CLI command.

Workaround: Performing a **shut** command followed by a **no shut** command on the PVC will reactivate it.

Alternate Workaround: Disable OAM management.

- CSCed00334

  Symptoms: A router crashes on configuring an ATM ESI address.

  Conditions: This symptom is observed when a deleted subinterface is reused.

  Workaround: There is no workaround.

- CSCed01613

  Symptoms: The data path may be broken.

  Conditions: This symptom is observed on an interface of a CE router when L2TPv3 sequencing is configured for AAL5 over L2TPv3 (pseudo-wire type).

  Workaround: Disable L2TPv3 sequencing.

- CSCed02802

  Symptoms: A 1-port 10-Gigabit Ethernet line card may generate pause frames under an inbound heavy load if there is a bottle neck in the router, for example an egress line card. The pause frames may cause FCS errors at the remote end device.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(25)S2.

  Workaround: There is no workaround.

- CSCed02859

  Symptoms: During installation of a router on an OC-48 DPT/RPR ring, the ring became unstable, and 5 Cisco 12000 series routers reloaded, one reloading twice.

  Conditions: This symptom is observed on a mix of Cisco 12016 routers and Cisco 12416 routers that are running Cisco IOS Release 12.0(23)S3 3DES software.

  Workaround: There is no workaround.

- CSCed03096

  Symptoms: Shutting down the loopback 0 causes the 3xGigabit Ethernet (engine 2) line card to fail when it is configured with EoMPLS and VPN, and hardware multicast is enabled. This also happens on POS line cards and if a line card reload is done when multicast and VPN are both enabled.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed05344

  Symptoms: The Gigabit Ethernet port on a 10-port Gigabit Ethernet base card may be in the up/up state even though there are no cables plugged in.

  Conditions: This symptom is observed when the 10-port Gigabit Ethernet card has one EPA in the top slot and two ports on the EPA configured and enabled. Each time the router is booted, the Gigabit Ethernet port on the 10-port Gigabit Ethernet base card is in the up/up state.

  Workaround: There is no workaround.

- CSCed06014

  Symptoms: On a Cisco router, IPv6 traffic is counted under IPv4 counter on the Engine 4 POS line cards on the egress side when using the **show interface** *number* [**accounting**] command.

Conditions: This symptom is observed on a Cisco 12000 series router.

Workaround: There is no workaround.

- CSCed06105

  Symptoms: An RP may crash when a protected link is cut.

  Conditions: This symptom is observed on a Cisco 12000 series with an PRP that functions as a PE router with FRR, that protects VPN traffic over an PE-to-PE traffic engineering tunnel, and that has a Fast Reroute SNMP trap enabled.

  Workaround: Disable the Fast Reroute trap.

- CSCed07673

  Symptoms: The copy function from TFTP into the running configuration file may fail even though it appears as though the copy function has succeeded. An error message similar to the following may be displayed:

  ```
  Simultaneous configs not allowed: locked from vty0 (10.1.11.111)
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that has a single Route Switch Processor (RSP) when the following conditions are present:

  - The **service multiple-config-sessions** global configuration command is enabled on the router.
  - There is one vty session that is in configuration mode.
  - You enter the **copy tftp running-config** privileged EXEC command from another vty session.

  Workaround: There is no workaround.

- CSCed08096

  Symptoms: A line card may crash because of a timeout during the “get_stat” operation.

  Conditions: This symptom is observed on a 4-port OC-12 ATM ISE line card that functions under extreme conditions such as cold temperatures and high voltages.

  Workaround: There is no workaround.

- CSCed08366

  Symptoms: Multicast traffic stops flowing via an ATM interface.

  Conditions: This symptom is observed when detaching and attaching the PVC to an ATM interface while sending multicast traffic over the PVC.

  Workaround: After removing and attaching the PVC, enter the **shutdown** command followed by the **no shutdown** command on the interface.

- CSCed08696

  This umbrella caveat affects the behavior of path triggers, and of Automatic Protection Switching (APS) with PPP and Frame Relay (FR) encapsulation.

  - CSCec70879

    Symptoms: Cisco 12000 series POS APS interfaces do not permit the configuration of path trigger specifications on APS interfaces.

    Conditions: This symptom is observed on a Cisco 12000 series router.

    Workaround: There is no workaround.

  - CSCdu45201:

    Symptoms: When the **encapsulation ppp** interface configuration command is configured on Cisco 12000 series Packet-over-SONET (POS) APS interfaces, some APS operations may result in an inappropriate protocol state. This situation may stop all traffic flow through the APS pair or duplicate all packets.

    Conditions: This symptom is observed on a Cisco 12000 series router.

    Workaround: There is no workaround.

  - CSCec72228:

    Symptoms: When the **encapsulation frame-relay** interface configuration command is configured on Cisco 12000 series POS APS interfaces, some APS operations may cause interfaces (that have been selected by APS) to be set to “protocol down” by FR. This behavior can result in the loss of all traffic over the APS pair.

    Conditions: This symptom is observed on a Cisco 12000 series router.

    Workaround: There is no workaround.

- CSCed09364

  Symptoms: Ping packet that are larger than 1498 bytes may not pass successfully through a multilink interface.

  Conditions: This symptom is observed when a bridge group is configured on a multilink interface. The symptom does not occur when there is no bridge group on the multilink interface.

  Workaround: Change the maximum transmission unit (MTU) on the multilink interface from the default value of 1500 bytes to 1498 bytes.

- CSCed10778

  Symptoms: A failure of an active Route Processor (RP) may cause the standby RP to fail also.

  Conditions: This symptom is observed in Cisco 12000 series Internet routers.

  Workaround: There is no workaround.

- CSCed10965

  Symptoms: All line cards may crash due to an IPC timeout or fabric ping timeout.

  Conditions: This symptom is observed on a Cisco 12000 series with a PRP under heavy traffic conditions. The output of the **show controllers psar** command shows excessive error events (e.g. free queue empty events).

  Workaround: There is no workaround. The fix for this DDTS adds the new **show monitor event-trace psar** command to show any bursty error events that are traced but not visible in the output of the **show logging** command.

- CSCed11730

  Symptoms: It is not possible to use Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) virtual MAC addresses when HSRP or VRRP is configured over a port channel interface.

  Conditions: This symptom is observed on a Cisco 10720 router but may also be observed on other Cisco platforms.

  Workaround: Use the burn-in address (BIA) MAC address when you configure HSRP or VRRP over port channel interfaces.

- CSCed11793

  Symptoms: The output queue of a Gigabit Ethernet port may become stuck, preventing traffic from leaving the interface.

  Conditions: This symptom is observed on the Gigabit Ethernet port 0/1 (gig0/1) of a Network Processing Engine NPE-G1 (NPE-G1) that is installed in a Cisco 7200 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

  Alternate Workaround: Reload the router.

- CSCed12818

  Symptoms: A Cisco 12000 series Engine 3 (E3) line card does not forward traffic to networks that are not specifically present in the routing table.

  Conditions: This symptom is observed if a default route is learned by way of the **ip default network** global configuration command. If routes are learned by way of a default route, this symptom is not present.

  Workaround: There is no workaround.

- CSCed13350

  Symptoms: A ping from an interface of a Cisco 7500 series that functions as a PE router to a CE router may fail.

  Conditions: This symptom is observed on a Cisco 7500 series that runs IMPLS and that has CEF switching enabled.

  Workaround: Enter the **ip route-cache** command on the affected interface.

- CSCed13818

  Symptoms: The MPLS label capability is not registered by BGP peers that are configured to exchange MPLS labels over IPv4 BGP sessions. This results in labels not being exchanged (or allocated where necessary) by the BGP peers.

  Conditions: This symptom is observed when BGP peers are configured to exchange MPLS labels over IPv4 BGP sessions.

  Workaround: There is no workaround.

- CSCed14064

  Symptoms: On a Cisco router that is configured with LLQ, there is queueing on the real time queue.

  Conditions: This symptom is observed on a Cisco 10000 ESR that is configured with LLQ.

  Workaround: There is no workaround.

- CSCed14083

  Symptoms: When you remove a subinterface with an MQC service policy, a router may crash.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S.

  Workaround: Remove the service policy before you remove the subinterface.

- CSCed14287

  Symptoms: When you run Field Diagnostics on a 2xOc192 POS line card, a message appears stating that the card is not supported.

  Conditions: This symptom is observed when you Field Diagnostics on a 2xOc192 POS line card on a Cisco 12000 series that runs a release before Cisco IOS Release 12.0(27)S.

Workaround: There is no workaround. Ensure that you use the latest Field Diagnostics image that supports the 2xOc192 POS line card.

- CSCed15797

  Symptoms: On Engine 2 (E2) n-port OC3 line cards for the Cisco 12000 series router, the **pos delay triggers path** router configuration command does not implement the specified delay. This results in the link being brought down for Path Alarm Indication Signal (PAIS) or Path Remote Defect Indication (PRDI) defects whose duration is smaller than the specified delay time.

  Conditions: This symptom is observed in all releases of Cisco IOS Release 12.0 ST and in all releases of 12.0 S beginning with Release 12.0(22)S.

  Workaround: There is no workaround.

- CSCed15913

  Symptoms: An Engine 0 12xE3 line card may reload when changing the MTU on an Engine 2 3x1GE line card.

  Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(26)S.

  Workaround: Ensure there is no traffic going through the Engine 0 12xE3 and Engine 2 3x1Ge line cards when attempting to change the MTU.

- CSCed16284

  Symptoms: Packet precedence on transmit is incorrectly remaining the same (set-prec-transmit action is not working).

  Conditions: Interface configuration includes Rate Limiting that sets precedence to change on transmit with rate limit command that includes conform-action set-prec-transmit 1 and exceed-action set-prec-transmit 0. The Packets received are initially at Precedence of 2, but instead of changing to either a Precedence of 1 or a Precedence of 0, all packets are transmitted still at a Precedence of 2.

  Workaround: There is no workaround.

- CSCed16989

  Symptoms: The standby RP of a Cisco 7500 series may reload.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an ATM local-switching autoprovisioned L2 transport PVC when you enter the **connect** command.

  Workaround: Manually configure an L2 transport PVC before you enter the **connect** command.

- CSCed19210

  Symptoms: MLP bundles and their associated line protocol interfaces may flap, and the data path may be broken.

  Conditions: This symptom is specific to a Cisco 12000 series Engine 3 line card that supports MLP.

  Workaround: There is no workaround.

- CSCed20042

  Symptoms: A Cisco router may unexpectedly reload if IPv6 encounters a routing loop, and IPv6 CEF is enabled.

  Conditions: This symptom occurs under the following conditions:

  - IPv6 must be enabled
  - IPv6 CEF must be enabled

  - The IPv6 RIB must have recursive entries that form a loop, for example:

```
Router# show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
B   ::/0 [200/0]
     via 2::2
C   1::/64 [0/0]
     via ::, Ethernet0/0
L   1::2/128 [0/0]
     via ::, Ethernet0/0
C   2::/64 [0/0]
     via ::, Ethernet1/0
L   2::1/128 [0/0]
     via ::, Ethernet1/0
B   2001::/16 [200/0]
     via 2002::1
B   2002::/16 [200/0]
     via 2001::1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

    Note that 2001::/16 and 2002::/16 results in a recursion loop because 2001::/16 is accessible via 2002::/16 and 2002::/16 is accessible via 2001::/16.

  Workaround: Disable IPv6 CEF using the global configuration command **no ipv6 cef**.

- CSCed20379

  Symptoms: A 6-port CT3 line card crashed due to a Cache Parity Exception. The router will not reload.

  Conditions: This symptom occurs on a Cisco 12000 series router that is running Cisco IOS Release 12.0(23)S3 image c12kprp-p-mz.

  Workaround: There is no workaround.

- CSCed21111

  Symptoms: There is no console response from the primary or secondary route processor.

  Conditions: This symptom occurs after the **redundancy force-failover main-cpu** EXEC command is sent for the second cutover.

  Workaround: There is no workaround.

- CSCed22100

  Symptoms: An ingress Engine 4 plus POS line card may drop fragmented packets.

  Conditions: These symptoms occur in an IP-to-IP scenario under the following conditions:

  - The IP packet size is 28 bytes.

  - An Engine 4 plus GE linecard is present in the path before the packets reach the Engine 4 plus POS line card.

  Workaround: There is no workaround.

- CSCed22224

  Symptoms: On a Cisco 10000 series with a 4-Port Channelized STM-1/OC-3 or 1-Port Channelized OC-12/STM-4 line card, when you enter the **shutdown** command followed by the **no shutdown** command on the SONET controller, the serial interfaces that are configured under this controller stay down until you enter the **no shutdown** command on each individual serial interface.

  Conditions: This symptom is observed when the line card has au-4-tug3 controllers configured. The au-3 mapping appears to work correctly.

  Workaround: There is no workaround. Bring up the serial interfaces by entering the **no shutdown** command on each individual serial interface.

  Further Problem Description: The symptom also occurs when you enter the **shutdown** command on the au-4-tug3 controller.

- CSCed22358

  Symptoms: A Cisco 12000 series that is running Cisco IOS Release 12.0(26)S with an Engine 3 POS line card (OC48X/POS-SR-SC), and possibly other Engine 3 line cards, may forward packets out of an incorrect interface. This behavior can been seen by looking at the hardware CEF entry on this input line card:

  ```
  execute-on slot x show ip hardware-cef a.b.c.d
  ```

  where a.b.c.d is the destination ip

  The output will look similar to this, where the CEF lookup is null:

  ```
  LC-Slot0#sh ip hardware-cef a.b.c.d
  Leaf FCR 2 0x784C6FC0 found 2 deep
  alpha ip loadbalance: 0x78198D00 - lbl not equal. cef lookup NULL
  ```

  After clearing the route:

  ```
  LC-Slot0#sh ip hardware-cef "a.b.c.d"
  Leaf FCR 4 0x784C6FC0 found 2 deep
  Fast Adjacency:
  alpha adjacency: 0x701E8280
  [0-7] oi 0x4019100 oq 4000 in 15 ab 0 hl 20 gp 11 tl 0 loq BC01 15/0 mtu 4470
  packets 1750013440 bytes 776867999767

  Output Queue / Local Output Queue Bundle:
  [0-7]   output queue 0x4000 local output queue 0xBC01
  ```

  This problem can lead to packets being dropped due to the creation of a loop and the TTL expiring on the packets.

  Conditions: This symptom is observed on a Cisco 12000 series that is running Cisco IOS Release 12.0(26)S with an Engine 3 POS line card (OC48X/POS-SR-SC).

  Workaround: Change the routing so the packets do not enter via the Engine 3 line card or use a different Engine line card. Clearing the route resolves the problem only temporarily.

- CSCed22582

  Symptoms: The cbQosPoliceStatsTable MIB objects of the QOS-MIB may be missing.

  Conditions: This problem affects QoS statistics that are defined in the CISCO-CLASS-BASED-QOS-MIB

  Workaround: There is no workaround.

- CSCed22837

  Symptoms: A router may reload unexpectedly when packets are tag switched.

  Conditions: This symptom is observed when a Bridge-Group Virtual Interface (BVI) is created after the router has booted up, when IP packets are received through the BVI, and when these IP packets are forwarded as Multiprotocol Label Switching (MPLS) packets through another interface.

  Workaround: Disable tag switching on the BVI interface by entering the **tag-switching ip** interface configuration command followed by the **no tag-switching ip** interface configuration command.

- CSCed23567

  Symptoms: %IPCLC-3-INTRLVL error messages and tracebacks may be seen on an Engine 2 8xOC3 ATM line card. This situation may cause an 85-percent CPU utilization on the line card.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed23828

  Symptoms: L2 fragmentation does not happen for packets greater than the network Maximum Transmission Unit (MTU). Packets are dropped.

  Conditions: This symptom occurs when distributed Cisco Express Forwarding (dCEF) is enabled on an RSP.

  Workaround: Either turn dCEF off or configure the MTU to be equal to the network MTU on the customer edge (CE) routers.

- CSCed23900

  Symptoms: Features on an ISE-based line card may not work.

  Conditions: This symptom is observed when the line card is newly inserted into a Cisco 12000 series. Packet forwarding is not affected.

  Workaround: Reload the router.

- CSCed24020

  Symptoms: The IP multicast throughput in Cisco IOS Release 12.3(6)T is not as good as in Release 12.3(4)T.

  Conditions: This symptom is observed when more than 130 kpps of traffic is sent. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed24502

  Symptoms: Any Transport over Multiprotocol Label Switching (AToM)/Layer 2 Tunneling Protocol version 3 (L2TPv3) data packets that are received on a VLAN subinterface may be dropped when multicast is enabled on any other VLAN subinterface of the same physical interface.

  Conditions: This symptom is observed on a Cisco 2600 series and Cisco 3600 series when Xconnect is configured on yet another VLAN subinterface of the same physical interface. However, the symptom is platform independent.

  Workaround: Disable multicast on the physical interface or on its subinterfaces that have Xconnect configured. If this is not an option, there is no workaround.

- CSCed24858

  Symptoms: Flow control information is not sent to the line card correctly, which causes errors in flow control issues.

Conditions: When a VC is created, if the VC goes down or is inactive during the first 60 secs, the flowbit information may not be updated correctly on the line card.

Workaround: Create another VC. This will cause IOS to go through all of the active VCs and update all their flowbit information.

- CSCed25921

  Symptoms: Traffic loss and tracebacks may occur on an Engine 2 (E2) 4xOC12 line card when diagnostics are run on the backup clock scheduler card (CSC).

  Conditions: This symptom is observed on a Cisco 12012 router when the backup CSC is in slot 17 of the router.

  Workaround: There is no workaround.

- CSCed26242

  Symptoms: An Engine 3 QOC12 LC configured with multicast VPNs may drop or punt traffic to the RP. This may happen when the **mdt data** *group-address-range wildcard-bits* **threshold** *threshold-value* command is configured in VRF configuration mode.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: Remove the **mdt data** *group-address-range wildcard-bits* **threshold** *threshold-value* command from the VRF configuration.

- CSCed26664

  Symptoms: The output packet counters on an interface may be incorrect. Depending on the Cisco IOS release, they may show either a very large or unexpected value.

  Conditions: The output packet counters get corrupted by clearing the interface counters followed by reloading the PXF microcode. The commands are the **clear counters** command followed by the **microcode reload pxf** command.

  Workaround: Issue another **clear counters** command.

- CSCed28122

  Symptoms: An ATM interface configuration may become corrupted.

  Conditions: This problem may be encountered when ATM subinterfaces are deleted and subsequently reenabled or when an interface is unplugged and then reinserted.

  Workaround: There is no workaround.

- CSCed28565

  Symptoms: OAM cells are not sent when you configure the **oam-pvc manage** command on a PVC.

  Conditions: This symptom is seen on a 4 port OC-3 ATM ISE line card when distributed OAM is enabled (which is the default mode of operation).

  Workaround: Disable distributed OAM by entering the **no atm oam distributed interface configuration command.**

- CSCed28604

  Symptoms: Enabling autonegotiation on an E1 Gigabit Ethernet interface causes the standby route processor (RP) to fail.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(26)S.

  Workaround: Stop the traffic, enter the **shutdown** command on the interface, configure autonegotiation on the interface, enter the **no shutdown** command on the interface, and resume the traffic.

- CSCed29514

  Symptoms: A Cisco 7200 series NPE-G1 built-in GE (SBeth) MAC filter may accept NULL DAs (00-00-00-00-00-00). This unintentional behavior may pose a denial of service security risk in customer environments when their networks are flooded with NULL DAs.

  Conditions: This symptom is observed when NULL DAs are presented to an NPE-G1 GE interface. This situation may be either a third-party vendor product flaw or a third-party vendor documentation error. (The third-party vendor documentation states that NULL DAs may be used for unused MAC Filter entries, implying that they are not accepted.)

  Workaround: There is no workaround.

- CSCed29519

  Symptoms: An Engine 4+ GE line card stops forwarding Multiprotocol Label Switching (MPLS) VPN traffic.

  Conditions: This symptom occurs after Cisco Express Forwarding (CEF) on the line card is cleared.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the line card.

- CSCed29776

  Symptoms: The **traffic-shape** command may disappear from the running configuration after an HA switchover and it is not possible to reconfigure it on the newly active route processor.

  Conditions: This symptom is observed when the **traffic-shape** command is configured on an interface of an Engine 4+ line card on a Cisco 12000 series that has multiple route processors installed and when an HA switchover occurs.

  Workaround: Reload the router and reconfigure the **traffic-shape** command.

- CSCed31579

  Symptoms: A SONET controller may enter the down state upon reception of an LRDI alarm, but the controllers and interfaces at the lower levels remain up. This situation causes traffic to stop.

  Conditions: This symptom is observed when an LRDI alarm is received and when only the SONET controller goes down. The SONET controller should remain up.

  Workaround: Remove the LRDI alarm. Doing so causes the SONET controller to go up, and traffic will resume.

- CSCed32081

  Symptoms: A BGP session may not be established across an Engine 2 1xOc48 SRP link.

  Conditions: This symptom is observed on a Cisco 12416 router that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCed32758

  Symptoms: A reload or online insertion and removal (OIR) of any line card on a Cisco 12000 series Internet router chassis with a 1+1 Automatic Protection Switching (APS) configuration between two CHOC-48 line cards may cause a “deadman timer expired” error. This may result in an incorrect switch working once the line card comes up.

  Conditions: This symptom is observed on a Cisco router with a channelized OC48 line card that is running the c12kprp-p-mz image of Cisco IOS Release 12.0(24)S4.

  Workaround: There is no workaround.

- CSCed33627

  Symptoms: A 3-port Gigabit Ethernet (GE) line card may show an BMA error, then run error recovery.

  Conditions: This symptom is observed on a Cisco 12008/40 router that is running Cisco IOS 12.0(23)S5, that is configured as an MPLS inter-AS ASBR, and that is also configured as a PE router. When you enter the **shutdown** command followed by the **no shutdown** command on a POS interface of an 8-port POS line card, the 3-port GE line card shows an BMA error.

  Workaround: There is no workaround.

- CSCed34184

  Symptoms: After performing a manual switchover on a dual PR router in SSO mode, the following traceback may be seen:

  ```
  %SYS-3-MGDTIMER: Uninitialized timer, timer delink
  ```

  In some cases, this situation may cause the RP to reload.

  Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed34642

  Symptoms: An Engine 4+ line card may generate errors after a router reloads.

  Conditions: This symptom occurs only when the line card is switching small packets (IP length ~28 bytes).

  Workaround: There is no workaround.

- CSCed34665

  Symptoms: The interface protocol is down when keepalive is configured, and the **speed 100** interface configuration command does no longer function.

  Conditions: This symptom is observed on a Cisco 10720.

  Workaround: Use the **speed auto** command, assuming that the connected device also supports this command.

- CSCed35573

  Symptoms: A ping does not go through for large packet sizes.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed36386

  Symptoms: When an interface that is configured with an IP address goes down while another interface is configured with the same IP address, traffic destined to this IP address may not be received by the interface that remains up.

  Conditions: This symptom is observed when CEF is enabled.

  Workaround: Flap the interface that is up. Doing so enables the interface to receive traffic for the IP address.

- CSCed37615

  Symptoms: A router may reload unexpectedly after renaming a policy-map the second time.

  Conditions: This defect may be observed if there are at least two policies configured.

Workaround: Avoid renaming the policy-map.

- CSCed37749

  Symptoms: Any Transport over Multiprotocol Label Switching (AToM) virtual circuits (VCs) may fail to come up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2 S and that is configured for AToM and Cisco Express Forwarding (CEF). The symptom may also occur in Release 12.0 S.

  Workaround: Toggle the CEF configuration; that is, remove CEF and reconfigure CEF.

- CSCed39059

  Symptoms: The tag forwarding table for a line card on Cisco platforms that have distributed (i.e. linecard based) forwarding, such as the Cisco 7500 Series and the Cisco 12000 Series, may not have complete entries even though the Route Processor (RP) does. This results in ingress tagged traffic being dropped for the missing tag forwarding entries.

  Conditions: This symptom is observed on Cisco platforms that have distributed (i.e. linecard based) forwarding in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment with a provider edge (PE) router to customer edge (CE) router link.

  The problem is more likely to happen if the PE to CE link experiences quick flaps of an interface (i.e. goes down and come back up in a very small amount of time (e.g. 2 sec)). Although this can happen on any linecard, this situation is more likely to happen on the Engine 3 (E3) channelized OC-48 line cards due to its quick flapping behavior.

  Note: There are additional prerequisites for this bug to happen. These are:

  – The defect affects routers that are: (a) MPLS VPN PE routers or (b) routers that exchange labels for ipv4 BGP routes.

  – For (a) there should be recursive routes on the PE that go over the PE-CE link (this could be either BGP learnt recursive routes or static recursive routes). Also, these recursive routes have the link's CE side ip address as their nexthop.

  – There should be a less specific route to get to the nexthop (this can be a default route). This applies for (a) and (b).

  Workaround: There is no workaround.

- CSCed39106

  Symptoms: Removal of the primary CSC from a Cisco 12816 router (when all 5 fabric cards are present in the router), stalls the active RP for about 10 minutes and brings down standby RP to ROMMON prompt.

  Conditions: This symptom is observed on a Cisco 12816 router.

  Workaround: Do not do an OIR of the primary CSC.

- CSCed40547

  Symptoms: A Cisco 7500 router may reload when dMLFR interface(s) is/are configured.

  Conditions: This problem can occur only when distributed CEF switching is disabled globally on the router. The following command can cause this issue to occur:

  ```
  Router(config)# no ip cef distributed
  ```

  Workaround: Do not disable distributed CEF switching on the router, as dMLFR works only when distributed CEF switching is enabled.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

- CSCed41067

  Symptoms: When the cache is lost, a router correctly detects that the cache is no longer available, but HTTP requests are still forwarded to the cache.

  Conditions: This symptom is observed on a Cisco 7500 series with dCEF enabled.

  Workaround: Disable dCEF.

- CSCed41231

  Symptoms: An alignment error may cause a Cisco router to reload unexpectedly.

  Conditions: This symptom is observed under rare conditions (an “extreme corner case”) on a MIPS-based Cisco platform or on a Versatile Interface Processor (VIP), port adapter, or line card that contains a MIPS processor. The symptom is not release-dependent and may occur in all Cisco IOS releases.

  Workaround: There is no workaround.

  Further Problem Description: All 7500 VIPs and 7200 NPEs use MIPS based processors. Additional platforms that use MIPS processors are:

  2691,3620,3631,3640,3660,3725,3745,4500,4500-M,4700,4700-M,AS5300,AS5400,AS5450, AS5800 Router Shelf,AS5800 System Controller (3640 based),7120,7140,UBR7100, UBR7200 - All NPEs,7301,7304,7400,6500 MSFC,6500 MSFC2,7600 MSFC,7600 MSFC2, 10000,UBR10012,12000 GRP, most (if not all) 12000 line cards.

- CSCed42587

  Symptoms: When sending 10 packets from AGT-SRC to AGT-Dest with TTL set to 3 on all packets, the first packet is dropped.

  Conditions: This symptom occurs under the following conditions:

  - Applies only to E2 LCs.
  - Interface with ACL rule with the “log” option
  - Packets with TTL of 3

  Workaround: Remove the “log” option from the ACL rule.

- CSCed43228

  Symptoms: On a Cisco 12000 series router with 2 GRPs which support SSO mode (Cisco IOS Release 12.0(24)S and later), when any Engine3 (E3 aka ISE) card is inserted after bringing up both GRPs in SSO mode, the applied service policy which has WRED configured on this interface, does not sync with standby GRP.

  Conditions: The problem only happens for any E3 card that was not in the chassis when the secondary RP booted. This will be the case when adding a new E3 LC to an already running system and configuring it for the first time. E3 cards that were in the chassis by the time the secondary RP finished booting will not exhibit this behavior.

  Workaround: Reload the secondary RP.

- CSCed43829

  Symptoms: Random Early Detection maintains an average length of the outbound queue of a class of traffic, and randomly discards newly arriving packets when the average falls within the configured range. A Cisco 10000 series router may contain an error in the average queue length computation which makes Random Early Detection too sensitive to the instantaneous queue length.

  Conditions: This problem is seen on a Cisco 10000 series routers that runs Cisco IOS Release 12.0(27)S but may also occur in earlier releases.

  Workaround: There is no workaround.

- CSCed44319

  Symptoms: A file that is copied to an ATA disk may become corrupted.

  Conditions: This symptom is observed on any Cisco IOS image that contains the fix for CSCdz27200. The problem does not occur on a disk that is formatted with 16 or less sectors/cluster.

  Workaround: Use an ATA disk that is formatted with 16 or less sectors/cluster. The **show disk all** command indicates how many sectors are configured per cluster.

- CSCed44793

  This caveat consists of two separate systems, conditions, and workarounds.

  Symptoms 1: A router may reload after a switchover to the standby processor.

  Conditions 1: This symptom is observed on a Cisco Route Switch Processor (RSP).

  Workaround1: There is no workaround.

  Symptoms 2: After a switchover to a standby processor, the indices of the interfaces in the system may be changed by mistake. This may cause problems with forwarding packets and may cause other inconsistencies.

  Conditions 2: This symptom is observed on a Cisco 12000 series.

  Workaround 2: There is no workaround.

- CSCed45093

  Symptoms: IP routing protocols may not stage on multilink PPP (MLP) interfaces on an ISE channelized OC-12 line card.

  Conditions: This problem is specific to an ISE channelized OC-12 line card and MLP interfaces.

  Workaround: Use static routes.

- CSCed45460

  Symptoms: The **hw-module slot** *slot-number* **ip multicast hw-accelerate source-table size 4096 offset 0** command is not synced to a standby RP if a line card is reloaded while the standby RP is booting.

  Conditions: Symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

  Workaround: Wait until the standby RP is fully operational before entering the above-mentioned command.

- CSCed45643

  Symptoms: An Engine 2 GE line card may not accept an MQC service policy.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCed45698

  Symptoms: Unused ports on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may flap even when they are not processing any traffic.

  Conditions: This symptom is observed when there is congestion on used ports of the PA-MC-STM-1 and when a committed access rate (CAR) is configured on these used ports.

  Workaround: There is no workaround.

- CSCed45746

  Symptoms: Several prefixes for non-redistributed connected interfaces in different VRFs may be partially bound to the same MPLS-VPN label, thus disrupting traffic bound to one or more of these VRFs.

  Conditions: This symptom can occur on a Cisco router that runs Cisco IOS Releases 12.2, 12.2T, 12.0S, 12.3 after the VRF interfaces have flapped. The symptom may occur in all code levels of these releases.

  Workaround: Clear the routes in the VRFs in sequence.

- CSCed46184

  Symptoms: VPN sessions may not be established.

  Conditions: This symptom is observed in an Xconnect configuration when a CFI interface goes down after the VPN service is being established. This is a timing issue.

  Workaround: Remove and reconfigure Xconnect.

- CSCed46669

  Symptoms: On a Cisco 12000 series in a dual-RP (GRPs or PRPs) SSO mode, when certain configuration commands are typed such as a nested **policy-map** command, the standby RP may crash. While the RP reboots after the crash, it is not available to perform its standby function.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(22)S or a later release. A nested **policy-map** command can cause this problem. In general, any configuration command that uses a large amount of processor stack space, such as the nested **policy-map** command may, may cause the standby RP to crash.

  Workaround: There is no workaround.

- CSCed46747

  Symptoms: After an SSO and before a standby RP is completely up, when you perform and OIR of line cards, a configuration synchronization failure may occur and the standby RP may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S when you perform an OIR of an 8-port Packet-over-SONET OC-3c/STM-1 single mode line card and a 4-port ISE Packet-over-SONET OC-12c/STM-4 single mode/IR SC connector line card.

  Workaround: Perform an OIR of these line cards after the standby RP is up.

- CSCed46785

  Symptoms: A line card may reload when a policy map is removed.

  Conditions: This symptom is observed when the policy map is child policy map of a policy map that is attached to a Frame Relay DLCI or ATM PVC.

  Workaround: Remove the service policy from the Frame Relay DLCI or ATM PVC before removing the policy map.

- CSCed46856

  Symptoms: Most multicast traffic is dropped if an ingress interface is an interface of an E4+ line card and NetFlow is configured.

  Conditions: This symptom occurs when multicast traffic is forwarded down a shared tree, for example, forwarded by (*, g).

  Workaround: Either unconfigure NetFlow or disable the SPT threshold to move to the shortest path tree.

- CSCed47409

  Symptoms: In Cisco IOS software that is running Multiprotocol Label Switching (MPLS), a router may reload after accessing a freed Label Information Base (LIB) entry. When the symptom occurs, an error message similar to the following is likely to precede the reload:

  ```
  %TIB-3-LCLTAG: 10.10.10.10/10.10.10.10, tag advert; unexpected tag state=13
  ```

  Conditions: This symptom is observed when a very uncommon timing of a Label Distribution Protocol (LDP) events occurs. The symptom may occur with LDP or Tagswitching Distribution Protocol (TDP).

  Workaround: There is no workaround.

- CSCed47967

  Symptoms: The line protocol may be in a DOWN state on the Ethernet interface of a Cisco 7206VXR with an NPE-400 and a 7200-I/O-GE+E I/O controller when the interface of the connected device is set to 10-Mbps operation. Additionally, the output of the **show controller e0/0** command may indicate that the hardware is set to an incorrect speed.

  Conditions: This behavior appears to be limited to the 7200-I/O-GE+E I/O controller and occurs consistently upon bootup.

  Workaround: Configure the speed of the interface of the connected device to 100 Mbps (both full-duplex and half-duplex settings will work).

- CSCed48824

  Symptoms: A router may crash when you remove a VLAN subinterface while traffic is being forwarded out of this subinterface.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: Ensure that no traffic is forwarded out of the subinterface before you remove it.

- CSCed48941

  Symptoms: A Cisco MGX 8800 series Route Processor Module XF (RPM-XF) may crash and generate the following error message:

  ```
  No memory for XCM tempbuffer logged
  ```

  Conditions: This symptom is observed on an RPM-XF that functions as a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when you enter the **clear interface sw1** command multiple times on the RPM-XF.

  Workaround: There is no workaround. The fix for this caveat is also integrated in images that support the Cisco 10000 series, such as Cisco IOS Release 12.0 S.

- CSCed49303

  Symptoms: A Cisco 12000 series that runs 12.0(25)S2 may report the following log message:

  ```
  SLOT 1: %SYS-3-CPUHOG: Task ran for 2052 msec (1/1), process = CEF LC IPC
  ```

```
Background, PC = 400DC728.
-Traceback= 400DC730 40DBFE60 40DBFFD4 40DC0B14 400C5A04 400C59F0
```

Conditions: This symptom is observed when the default route gets updated to Engine 3 line cards and is reported by these line cards as seen above. This situation may happen after an interface flap or a routing update elsewhere in the network.

To determine if your line card is an Engine 3 line card, enter the **show diag** *slot-number* EXEC command, in which the *slot-number* argument is the slot number that reports the message). In the command output, you will see "L3 Engine: 3" for Engine 3 line cards.

Workaround: There is no workaround.

- CSCed49539

  Symptoms: Field diagnostics may enable fabric FPGA loopback bits, causing a line card to remain off the fabric.

  Conditions: This symptom is observed on a Cisco 12400 series that runs Cisco IOS Release 12.0(27)S.

  Workaround: Enter the following commands for all fabric slots:

  test mbus write *slot* **22000 FF test mbus write** *slot* **22001 FF**

- CSCed49733

  Symptoms: The Cisco 10720 microcode will be reloaded upon reception of certain malformed MPLS packets.

  Conditions: An MPLS packet where the topmost label is an MPLS Aggregate Label (for either IPv4 or IPv6) and this label does not have the EOS bit set (that is, it is not the only label) will cause the reload.

  Workaround: There is no workaround.

  Further Problem Description: This should be an extremely rare situation as such packets are not allowed in MPLS, that is, IPv4/IPv6 aggregate MPLS labels must always be the only label on the received label stack and therefore they must always have the EOS bit set. Reception of such a packet implies that some other network element has generated an invalid MPLS packet.

- CSCed50426

  Symptoms: All multicast packets are dropped with a VRF-lite configuration.

  Conditions: This symptom occurs when MVPN is set up in a VRF-lite configuration.

  Workaround: There is no workaround.

- CSCed50510

  Symptoms: An IPC crash may be seen on a standby RP while upgrading from the gsr-p-mz image of Cisco IOS Release 12.0(25)S1 to the gsr-p-mz image of Cisco IOS Release 12.0(27)S. Tracebacks and error messages "%IPCGRP-3-UNKNOWNCMDMSG:" and "%IPCGRP-3-SYSCALL:" may be seen as well.

  Conditions: This symptom is observed on a Cisco 12416 router when following the recommended upgrade procedure.

  Workaround: There is no workaround.

- CSCed50514

  Symptoms: A Cisco router reloads with an unexpected exception and tracebacks.

  Conditions: This symptom occurs when a serial interface is configured and you try to remove the AUG controller. See the following example:

```
router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# cont sonet 3/0/0
router(config-controller)# no aug cont
router(config-controller)# no aug controller
router(config-controller)#
```

Workaround: There is no workaround.

- CSCed51139

  Symptoms: A Cisco 12000 series router with an HA configuration (dual RP redundancy) and with GE line cards which are using channel groups, might not be pingable after a redundancy switchover. From the interface, the directly connected device can be pinged, but from the same device, the interface cannot be successfully pinged.

  Conditions: The problem is specific to a Cisco 12000 series router that is running Cisco IOS 12.0 S. The router must have an HA configuration (dual RPs). Also, channel groups must be configured (note: even if the channel groups are not assigned to a particular Gige interface, the problem can still occur). Finally, a link flap needs to occur on the channel group interface before the redundancy switchover is done to bring on the problem.

  Workaround: Enter the **shut** command followed by the **no shut** command on the interface.

  Further Problem Description: The group channel feature is new and was released for the first time in Cisco IOS Release 12.0(26)S1 so that is where the exposure is.

- CSCed51371

  Symptoms: Intermittent packet drops occur when you ping the VRF loopback/interfaces on a PE router from an attached PE router. The VPN transit traffic intermittent drops occur also on packets that exceed the MTU size.

  Conditions: This symptom is observed on a Cisco 12000 series 3-port GE and 4-port GE line card that are installed in a Cisco router that functions as a PE router and that is connected to another PE router via an L2 switch. The problem occurs when a VRF is configured on a subinterface that faces the L2 switch.

  Workaround: Remove the VRF from the subinterface that faces the L2 switch.

- CSCed51610

  Symptoms: A Cisco 12000 series Engine 4+ line card is unable to originate ICMP echo reply packets. ICMP packets transiting the router are correctly transmitted.

  Conditions: This symptom occurs when the **rate-limit**, MQC **set**, or MQC **police** command is configured on the interface in the output direction.

  Workaround: There is no workaround.

- CSCed51664

  Symptoms: Gigabit Ethernet interfaces on a Network Processing Engine G-1 (NPE-G1) may not accept packets with long MPLS headers. This situation may decrease the performance of some network environment such as an Ethernet over MPLS (EoMPLS) environment.

  Packets with a size that exceeds the maximum MTU in the output of the **show controller gigabitethernet 0/x** command may be dropped.

  Conditions: This symptom is observed on a Cisco 7200 series.

  Workaround: Increase the MTU at the interface level.

- CSCed52163

  Symptoms: When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as “OID not increasing” may occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured.

  Conditions: This symptom is observed under either one of the following two conditions:

  – An SNMP HSRP query triggers a loop in the getnexts. Some MIB browsers catch this, and exit with a message stating “OID not increasing”.

  – A scaling problem may occur with HSRP when there are a high number of tracked interfaces. For every standby track statement, every interface is tested to see if it is an HSRP tracked interface. No defined thresholds have been identified and tested that qualify when this scaling problem may occur. The more interfaces there are configured, the greater is the possibility that the problem occurs.

  Workaround: Do not initiate an SNMP query for HSRP.

  Alternate Workaround: Enter the **snmp-server** global configuration command to specify which MIBs are available, as in the following example:

  snmp-server view *HSRP* **internet included**
  snmp-server view *HSRP ciscoHsrpMIB* **excluded**
  snmp-server view *HSRP ciscoHsrpExtMIB* **excluded**
  snmp-server community public view *HSRP RW 20*
  snmp-server community private view *HSRP RW 20*

- CSCed52578

  Symptoms: The MPLS packets are forwarded with a bogus label when they are sent out on a loadshared non-VRF MPLS enabled “Internet” interface from a VRF.

  Conditions: A static route for the VRF should be configured to reach the Internet, which would in turn be configured to recurse over 2 static routes to reach the next hop for the global Internet.

  Workaround: Shut down one of the interfaces to remove the load-sharing condition.

- CSCed54236

  Symptoms: A Cisco router reloads due to memory allocation problem when per packet load balancing is changed to default CEF load balancing.

  Conditions: This symptom is observed on a Cisco 7200 series router with a PA-4T serial adapter when the **service-policy output** *name* command is applied to this interface. The problem is observed in Cisco IOS Release 12.0(26)S1 and Release 12.0(27)S.

  Workaround: Use per-packet loadbalancing, remove the **service-policy output** *name* command, or replace the adapter with a PA-4T+.

- CSCed54262

  Symptoms: Memory allocation (MALLOC) failures may occur on a VIP, port adapter, or line card.

  Conditions: This symptom is observed on a Cisco router that has a scaled AToM configuration.

  Workaround: There is no workaround.

- CSCed54342

  Symptoms: A reload occurs that sends a Cisco 10000 series router into ROMMON state.

  Conditions: This symptom occurs after configuring CHOC3 interfaces and then performing the **shut** command followed by the **no shut** command. The reload sends the Cisco 10000 series router into ROMMON state.

Workaround: There is no workaround.

- CSCed54416

  Symptoms: A Cisco 12000 series may reload unexpectedly.

  Conditions: This symptom is observed when Multiprotocol Label Switching (MPLS) Fast Reroute (FRR) is configured.

  Workaround: There is no workaround.

- CSCed55962

  Symptoms: From a local customer edge (CE) router, you may not be able to reach or ping some prefixes (subnets) on a remote CE router over an Multiprotocol Label Switching (MPLS) network.

  Conditions: This symptom is observed in a cell-based MPLS network.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected subinterface that is connected to the local CE router. Doing so enables the Border Gateway Protocol (BGP) to run a scan again and repopulates the subnets in the Tag Forwarding Information Base (TFIB).

- CSCed56025

  Symptoms: A VIP, port adapter, or line card may reset.

  Conditions: This symptom is observed on a router that has a scaled AToM configuration.

  Workaround: There is no workaround.

- CSCed56092

  Symptoms: A standby GRP or PRP may keep resetting.

  Conditions: This symptom is observed on a Cisco 12000 series when you change releases from Cisco IOS Release 12.0(27)S to another release using the **hw-module standby reload** command and when the RPR mode is enabled.

  Workaround: Enter the **reload** command.

- CSCed56404

  Symptoms: On a Cisco 12000 series with link-bundling (port-channel) configured and the **snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart** command configured, if you configure the port-channel with minimum links that are greater that the actual links, the port-channel is forced down, and an SNMP linkdown trap is generated. However, if you correct the configuration so that the port-channel comes up, no linkup trap is generated.

  Conditions: This symptom is observed on a Cisco 12000 series router that runs Cisco IOS Release 12.0(26)S1.

  Workaround: There is no workaround.

- CSCed57281

  Symptoms: A router may log a CPUHOG message that is caused by the CEF reloader process.

  Conditions: This symptom is observed on a Cisco router when a VRF with more than 9000 routes is added to the configuration.

  Workaround: There is no workaround.

- CSCed57625

  Symptoms: An access control list (ACL) that has logging enabled may not work on a Fast Etherchannel (FEC) interface.

Conditions: This symptom is observed on a Cisco 10720 router running Cisco IOS Release 12.0(26)S or a later release.

Workaround: There is no workaround.

- CSCed57841

  Symptoms: When the error message "Info: Illegal normal burst size, increased to mtu size 4470" is generated on a channelized STM-1 MM PA, the VIP in which this PA is installed and the RSP may crash.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 when MQC is configured on the channelized STM-1 MM PA.

  Workaround: There is no workaround.

- CSCed59020

  Symptoms: An Engine 1 single port Gigabit Ethernet line card for a Cisco 12000 series router may reload unexpectedly on receipt of large amounts of "pause input" frames sent via flow control from a downstream device.

  Conditions: This symptom will occur only if the Gigabit Ethernet line card is forwarding large amounts of traffic to an overwhelmed downstream device that in turn sends "PAUSE" (XOFF) frames to the line card.

  Workaround: Disable flow control on the downstream device.

- CSCed60690

  Symptoms: Engine 4+ loadsharing does not work correctly for in a VPN imposition situation. The problem is not seen with Engines 0, 2 and 3.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S when traffic enters on a VRF interface and is loadshared over four links to the core. Traffic is loadshared over only two of the four links.

  Workaround: Use three-path loadbalancing.

- CSCed60987

  Symptoms: On a Cisco 7500 series with distributed CEF, connectivity between CE routers that are locally connected to the same interface may be broken.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or a later release when an output service policy is configured on the subinterface of one CE router but not on the subinterface of the other CE router. Traffic that is process-switched flows correctly between the CEs routers.

  Workaround: Configure a dummy output service policy on the subinterface that does not have an output service policy.

- CSCed61577

  Symptoms: After executing a forced switchover, the secondary processor returns only to COLD standby and not HOT standby.

  Conditions: This symptom is observed on a c10k-p10-mz image on a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCed61818

  Symptoms: Traffic forwarding stops when an egress CAR is configured on an Engine 0 interface.

Conditions: This symptom is observed on a Cisco 12000 series when IP-to-tag traffic arrives from an Engine 4+ line card and enters an Engine 0 line card that has a rate limit configured. The IP-to-tag traffic is dropped.

Workaround: Remove the rate limit from the Engine 0 interface, and enter the **shutdown** command followed by the **no shutdown** command on the interface.

- CSCed62375

  Symptoms: A misleading error message may be seen when a Stateful Switchover (SSO) of an RP occurs:

  ```
  ATM failed to create VC(VCD=0, VPI=0, VCI=0) on Interface ATM0/0/0
  ```

  Conditions: This symptom is observed on a Cisco platform that is configured for ATM.

  Workaround: There is no workaround.

- CSCed62637

  Symptoms: On a Catalyst 6500 series and a Cisco 7600 series FlexWAN module, the latency experienced by the priority class traffic varies with the load of the default-class traffic, and may exceed low-latency requirements when the link is oversubscribed with default-class traffic.

  Conditions: This symptom is observed when a FlexWAN module interface with a policy map that contains a class that is configured for low latency queueing is overloaded with default-class traffic.

  Workaround: Reduce the load of default-class traffic attempting to egress via the interface.

- CSCed62835

  Symptoms: A Cisco platform may crash after the following error is seen:

  ```
  SCHED: Stack for process CEF IPC Background running low, 48/6000
  %SYS-SP-6-STACKLOW: Stack for process CEF IPC Background running low, 48/6000
  ```

  Conditions: This symptom is observed with a recursive prefix with multiple next hops when these next hops match host routes that themselves are recursive prefixes and recurse through themselves.

  Workaround: Avoid recursion loops.

- CSCed63480

  Symptoms: The **hw-module** {**slot** *X*} command shutdown on a 4GE Eng3 that is using GEC may freeze a router during some time, bringing down line and protocols. Under certain circumstances, DCEF may also be disabled.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed64461

  Symptoms: Frame Relay local switching fails when RED is applied on a Cisco 12000 series router with a 2-port OC-3 channelized to DS1/E1 line card or a 6-port channelized T3 line card.

  Also, it is observed that the controller is reset when the following is removed/reapplied:

  ```
  rx-cos-slot all ToFabTable
     !
     slot-table-cos ToFabTable
       destination-slot 0 OC3
       destination-slot 1 GIGE
  ```

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: Perform the following steps:

Step 1) Remove the RED configuration.

Step 2) Reload microcode onto the line card (a 2-port OC-3 channelized to DS1/E1 line card or a 6-port channelized T3 line card).

Step 3) Reapply the RED configuration.

- CSCed65027

  Symptoms: When the MTU is toggled from 4470 to 9180 or 64, a 4xOC12 ATM line card may enter the “ERR CARV” state and does not recover. Even reloading the line card does not bring it back up.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0 S.

  Workaround: Reload the router.

- CSCed65584

  Symptoms: A VIP or FlexWAN may reload.

  Conditions: This symptom is observed on a Cisco 7500 series or Cisco 7600 series when a service policy is attached to a multilink Frame Relay interface.

  Workaround: There is no workaround.

- CSCed66001

  Symptoms: A %LINK-4-TOOBIG error message may appear on the console log of a Cisco 10000 series.

  Conditions: This symptom is observed when you send a ping or an L2TP packet across an MPLS interface that is configured for label imposition.

  Workaround: There is no workaround.

- CSCed66388

  Symptoms: A 4-port OC-12 ISE ATM card may crash when an L3 PVC is configured on a main interface, a service policy is attached to the L3 PVC, and there are F4 OAM VCs on the same the main interface. F4-OAM VCs are created when there are VP tunnels or layer 2 VPs that perform cell relay/cell packing.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed68376

  Symptoms: A router may enter a processing loop. This results in CPUHOG messages and may cause the router to reload.

  Conditions: This symptom is observed under some error conditions that are associated with configuring L2TPv3 tunnels (when the **xconnect** command is enabled).

  Workaround: There is no workaround.

- CSCed68763

  Symptoms: Engine 2 line cards may fail upon clearing BGP peers.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed69546

  Symptoms: When mixed channels are defined on a channelized OC-12 line card and these channels include DS3s, T1s, an DS0s, CEF/RIB inconsistency may occur, preventing traffic to be sent over the correct interfaces.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: When you delete interfaces or subinterfaces on the channelized OC-12 line card, ensure that the adjacency for the deleted interface is deleted before you configuring a new interface.

  This can be checked by entering the **show adjacency** or **show adjacency | include** *interface name* command. When the adjacency no longer appears in the output of the **show adjacency command, it is safe to add new interfaces.**

  Note that the **show adjacency** *type number* command cannot be used to get the required information.

  When deleting large numbers of interfaces, a delay of about 2 minutes should be enough to ensure that all of the adjacencies have been deleted.

- CSCed69722

  Symptoms: When a recursively resolved adjacency is “discard”(e.g., null0), a packet that is entering an Engine 3 4-port GE line card and that is destined to the “discard” adjacency is punted to the local line card CPU, causing high CPU utilization. Punting to the CPU is caused by a wrong adjacency that is populated for the corresponding route.

  Conditions: This symptom is observed on Engine 3 line cards that are installed in a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S1 or a later release.

  Workaround: There is no workaround.

- CSCed70822

  Symptoms: With four fabric cards (one CSC in slot 16 and three SFCs), after a power cycle, the line cards fail to come up and fabric ping timeouts occur.

  Conditions: This symptom is observed on a Cisco 12000 series and affects all E4 and E4+ cards.

  Workaround: Place a CSC card in slot 17. The fix for this caveat applies to all types of line cards (E0, E2, E3, E4 and E4+).

- CSCed71467

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: When a policy map is applied under an L2VPN (AToM: CRoMPLS) ATM PVC on a Cisco 12000 series Engine 3 ATM card, it is not possible to get class-map or policy-map statistics. When you enter the **show policy map interface** command, the following message is seen:

  ```
  Class statistics not available.
  ```

  This message is seen on a policy map without policing, and in this specific case, the policy map uses a class-default match and sets the MPLS EXP bits.

  Condition 1: This problem is seen when a policy map that does not include any policing is applied to a Cisco 12000 series Engine 3 ATM line card that is configured for AToM/L2VPN.

  Workaround 1: Enable policing to get the policy-map and class-map statistics.

  Symptom 2: If a policy map that involves policing is applied L2VPN (AToM: CRoMPLS) ATM PVC on a Cisco 12000 series Engine 3 ATM card, the policy-map statistics are available but the following incorrect message shows up at the top of the output of the **show policy map interface** command:

  ```
  NOTE: Statistics are aggregated for all the VC's in the subinterface
  ```

This statement is not true because the per VC policy-map statistics are available in the case of L2VPN PVCs on this line card.

Condition 2: This problem is seen when the same policy map as in Condition 1 is modified to include policing.

Workaround 2: There is no workaround.

- CSCed71490

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series router, traffic destined for the router may fail for about 10 minutes. This could cause routing protocol traffic to fail and routes to be lost. While the routes are still on the router, traffic will flow through the router with no issues.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0 S or Release 12.2(22)S and that is configured for SSO/Nonstop Forwarding (NSF) with a POS interface with Frame Relay encapsulation.

  Workaround: There is no workaround.

- CSCed72297

  Symptoms: Multiple SYS-3-CPUHOG error messages may be generated in the LDP process, eventually followed by a watchdog timeout crash:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
  (422/8),process = LDP.
  -Traceback= 6101DFC0 6102546C 61016FE4 6101CE24 6101728C 61017A30
  ...
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = LDP.
  -Traceback= 6085658C 6101DE48 6102546C 61016FE4 6101CE24 6101728C 61017A30
  ```

  After the router has reloaded, the output of the **show version** command indicates “Last reset from watchdog reset.”

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)S4 or Release 12.2(22)S and that is configured for MPLS LDP. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed72340

  Symptoms: Some MQC commands on 4xOC3 and 8xOC3 ISE line cards on Cisco 12000 series routers may result in a message similar to the following:

  ```
  % Service policy on FR sub-interface POS1/1.2 must be hierarchical.
  ```

  Due to the error, no policy is applied to the interface. Even though the running configuration has the policy on the interface, the policy will not take effect.

  Conditions: This symptom is observed on Cisco 12000 series routers.

  Workaround: There is no workaround.

- CSCed72764

  Symptoms: TE tunnel(s) fail to switch back to the explicit path option.

  Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0 S.

  Workaround: Continue to work either in the explicit path or in the dynamic path without shutting the link. Such a scenario is highly unlikely.

- CSCed73722

  Symptoms: On an Engine 3 4GE line card, traffic from a Catalyst switch to a Cisco 12000 series is not rerouted over the GEC link when disabling the physical interface on which the traffic is passing.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S1.

  Workaround: There is no workaround.

- CSCed73780

  Symptoms: An EPA-GE/FE-BBRD line card may experience repetitive crashes during normal operation.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S2 or 12.0(26)S1.

  Workaround: There is no workaround.

- CSCed74617

  Symptoms: After an RPR+ switchover, the output information of a tag adjacency is replaced by the output information of the corresponding IP adjacency. This situation causes MPLS traffic forwarding to stop.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that is configured with AToM VCs after a switchover in RPR+ mode has occurred.

  Workaround: There is no workaround.

- CSCed75108

  Symptoms: When an IP VRF is configured on an SDCC interface of a Cisco 10720 router, all MPLS packets which are to be forwarded through the SDCC interface are instead dropped by the PXF forwarding engine.

  Conditions: This problem is observed when setting up an MPLS-VPN in which the PE-CE interface is an SDCC interface on the Cisco 10720 router.

  Workaround: Disable the PXF forwarding path via the **no service pxf** command.

  Further Problem Description: The forwarding path must deal with MPLS packets that are destined for the SDCC interface by punting them rather than dropping them.

- CSCed75233

  Symptoms: A line card crashes when the CPK internal debug tool is enabled because of uninitialized data in the CPK debug code.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed75347

  Symptoms: CR and CPK VP policing is broken when a mux-ed PVC VCI range is above 4095.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed77178

  Symptoms: HSRP configured on the subinterfaces of an Engine 4+ GE line card may not work.

  Conditions: This symptom is observed when the subinterfaces are configured with VRFs.

Workaround: There is no workaround.

- CSCed77186

  Symptoms: The **password** [*encryption-type*] *password* (L2TP) command is lacking the automatic encryption function for nvgen.

  Conditions: This symptom is observed on a Cisco router when you attempt to configure the password that is used by a provider edge (PE) router for Layer 2 (L2) authentication.

  Workaround: If you require the automatic encryption function for nvgen, perform the following steps:

  1) Figure out the encrypted version of the text password, using the “username” and “service password-encryption” as a tool.

  2) In the **password** [*encryption-type*] *password* (L2TP) command, enter **7** for the *encryption-type* argument and the encrypted version of the password for the *password* argument.

- CSCed78519

  Symptoms: SCR continues to filter CLP(0) cells and tag CLP(1) cells when the CLP(0) filter is removed from the **class-map** command.

  Conditions: This symptom is observed when there are multiple PVCs and when the class map filters are globally removed.

  Workaround: There is no workaround.

- CSCed78847

  Symptoms: Cisco Express Forwarding (CEF) becomes disabled on a secondary Cisco 10000 series Performance Routing Engine (PRE) during a switchover.

  Symptoms: This symptom is observed after configuring 380 traffic engineering (TE) tunnels and checking that CEF is enabled on both the primary and secondary PREs and that all TE tunnel interfaces are up. Then, a forced switchover from the primary PRE to the secondary PRE is performed. When the secondary PRE comes up and it now the new primary PRE, all tunnel interfaces are down. The line is up but the protocol is down. Because CEF is disabled and not running, the tunnels do not function and no routing can occur.

  Workaround: Enable CEF on the primary PRE and enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces. Doing so enables the TE tunnels to come up.

- CSCed79804

  Symptoms: A CRoMPLS pseudowire may fail to come up.

  Conditions: This symptom is observed on a Cisco 12000 series when the disposition is changed from an Engine 4+ line card to an Engine 2 ATM OC-12 line card.

  Workaround: There is no workaround.

- CSCed80344

  Symptoms: When RPR is enabled, after configuring an event manager policy to force a switchover, the switchover does not take place after the policy is triggered.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCed81349

  Symptoms: A standby RP may fail when MPLS TE tunnels are configured.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

Workaround: There is no workaround.

- CSCed81415

  Symptoms: IS-IS, OSPFv2/OSPFv3 adjacencies, or BGP neighbourships across any of the interfaces of an Engine 2 line card may fail.

  Conditions: This symptom is observed on a Cisco 12000 series when the CPU of the Engine 2 line card is oversubscribed in terms of its maximum IPv6 packet-per-second forwarding rate (which is about 100 Kpps). (IPv6 traffic forwarding on an Engine 2 line card is performed by the CPU of the line card.)

  Workaround: There is no workaround.

- CSCed82102

  Symptoms: The **match atm-clp** command and the **match not atm clp** command may not be present.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCed82152

  Symptoms: An Engine 4+ line card may reset and generate errors.

  Conditions: This symptom is observed after a manual RP switchover in RPR mode.

  Workaround: There is no workaround.

- CSCed82185

  Symptoms: Tracebacks may occur in the CDP process on a dual-PRP router.

  Conditions: This symptom is observed after the router is manually switched over to the standby RP in RPR+ mode.

  Workaround: There is no workaround.

- CSCed82871

  Symptoms: Line card instability may occur when passing MVPN traffic on an Engine 3 line card with slowpath running, and then configuring hardware multicast while traffic is running.

  Conditions: This symptom is observed on a Cisco 12000 router acting as an MVPN decapsulation PE router with an Engine 3 Quad OC-12 line card forwarding multicast packets on a VRF interface.

  Workaround: There is no workaround.

- CSCed83044

  Symptoms: A standby RSP may reload with the following error message:

  ```
  %SYS-6-STACKLOW: Stack for process IPC Seat Manager running low
  ```

  Conditions: This problem happens on a Cisco 7500 series router that runs Cisco IOS Release 12.0(27)S with IOPS when RPR, RPR+ or SSO redundancy modes are configured and when certain ATM subconfiguration commands such as the **connect** command are executed on the active RSP.

  Workaround: There is no workaround.

- CSCed83256

  Symptoms: A Cisco 12000 series may hang when you enter the **no shutdown** or **atm ilmi-pvc** command.

Conditions: This symptom is observed on a Cisco 12406 that runs the grp-p-mz image of Cisco IOS Release 12.0(28)S and that is configured with dual GRPs and a 4-port OC-12 ATM ISE line card.

Workaround: There is no workaround.

- CSCed83434

  Symptoms: On a line card, the VPN prefixes in one VRF may be attached to another VRF.

  Conditions: This symptom is observed when more than one VRF is configured in nonalphabetical order and a when an RPR+ switchover occurs.

  Workaround: After configuring VRFs, reload the router before a switchover can occur.

- CSCed84331

  Symptoms: MPLS TE tunnel counters are inaccurate; the MPLS TE tunnel output rate counters may exceed the physical interface capabilities that the tunnel uses.

  Conditions: This symptom is seen on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S5 with an Engine 4 line card. This symptom may be observed by issuing the following commands in the following order:

  1. Enter the **show interfaces tunnel** *number* command. This command tells you the interface statistics for the tunnel.
  2. Enter the **show mpls traffic-eng tunnels** *tunnel-interface* command. This command tells you the physical interface the tunnel traverses.
  3. Enter the **show interfaces** *type slot/port* command. This command tells you the physical interface statistics.

  Workaround: There is no workaround.

- CSCed84474

  Symptoms: After an APS switch using channelized OC-12 line cards (channelized to DS-1), some Frame Relay interfaces may fail to carry traffic.

  Conditions: This symptom is observed on a Cisco 12000 series with an OC-12 line card (channelized to DS-1) with a linear APS configuration.

  Workaround: If an individual interface does not recover on its own, enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed84639

  Symptoms: Engine 3 line cards on a Cisco 12000 series router may not display outgoing flows in the NetFlow cache.

  Conditions: This symptom is observed when output Netflow in configured on these line cards.

  Workaround: There is no workaround.

- CSCed85073

  Symptoms: For MVPN traffic, multicast traffic streams are punted from the PXF to the RP. Normally, PXF does this when a new stream needs to be created. However in this case, PXF behaves as if the streams are not present even if the required (S,G)/(*,G) states exist.

  Conditions: This symptom is observed on a Cisco 10000 series when the VRF index of the VPN is higher than 255. This occurs when 255 or more VRFs are configured or when some VRFs are created and deleted many times. You can determine the VRF index by entering the **show ip vrf detail** command.

  Workaround: There is no workaround.

- CSCed85570

  Symptoms: When a POS card is shut down, the show facility status still indicates alarms. When a line card is shut, there should be no alarms for that card.

  Conditions: This symptom is observed on Cisco 10000 series.a POS line card.

  Workaround: There is no workaround; ignore the alarms in the show facility status, it is a display error.

- CSCed86596

  Symptoms: IPv4 multicast traffic may stop being forwarded when NetFlow is configured on an Engine 4+ interface.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the Cisco IOS Release 12.0 S when a (*,G) entry is used to forward IPv4 multicast traffic instead of a (S,G) entry.

  Workaround: There is no workaround.

- CSCed86694

  Symptoms: When APS is configured, traffic stops flowing after you perform an OIR on two line cards (each line card once).

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround. To reenable the traffic flow, reset both line cards at the same time (that is, one immediately following the other).

- CSCed86984

  Symptoms: CEF may become disabled on a VIP, port adapter, module, or line card because of a fatal error, and the following error message may be generated:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 2: Window did not open, LC to RP IPC is
  non-operational
  ```

  Conditions: This symptom is observed after an RPR+ switchover.

  Workaround: There is no workaround.

- CSCed89518

  Symptoms: MPLS IAS traffic may be punted the CPU of an Engine 2 line card.

  Conditions: This symptom is observed when an egress interface is flapped and the ingress POS-channeling interface is shut down in a topology in which the ingress POS-channeling interface connects to an ASBR that connect to the egress POS interface.

  Workaround: There is no workaround.

- CSCed89629

  Symptoms: A VIP4-80 may crash when you enter the **police** command for a policy map that is applied to an ATM subinterface PVC in the input direction.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or 12.0(27)S.

  Workaround: Do not enter the **police** command for a policy map that is applied to an ATM subinterface PVC.

- CSCed89760

  Symptoms: When a primary CSC switchover happens on a Cisco 12800 series, a line card may reset.

  Conditions: This symptom is observed when there is primary CSC switchover, either through a CLI command or a physically removal of the primary CSC.

Workaround: There is no workaround.

- CSCed89963

  Symptoms: A Cisco 12000 series may experience a block overrun and redzone corruption with a subsequent system reload or switchover as a result of incorrectly processing a corrupted packet. Error messages similar to the following may be observed:

  ```
  %GRP-4-CORRUPT: Corrupted packet, start_offset 96, length 65534, slot 9
  %SYS-3-OVERRUN: Block overrun at 53E4389C (red zone 00000000)
  ```

  Conditions: This symptom may be observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S and that has 1- or 3-port Gigabit Ethernet line cards installed.

  Workaround: There is no workaround.

- CSCed90701

  Symptoms: The packet queue size on an MLP bundle may be larger than necessary, which may manifest as two separate symptoms:

  – The scalability during configuration of multiple MLPPP interfaces is reduced because the router may run out of resources to allocate the packet queues.

  – The effect of congestion may be more severe as traffic that should have been dropped due to the queue overflow will not be dropped.

  Conditions: This happens after the reload of a Cisco 10000 series with a policy map attached to an MLP interface or when more links are added to an MLP interface.

  Workaround: After any MLP bundle change (either by configuration, bootup, or link failure) delete and reattach the service policy to the interface.

- CSCed90731

  Symptoms: The priority traffic on an MLP interface may exceed the configured bandwidth limits.

  Conditions: This symptom is observed on a Cisco 10000 series when new links are added to an MLP interface that already has a policy map with a priority class attached. The link addition may happen as result of a system bootup or a link flap, or a user may add more links to the bundle by configuration.

  Workaround: Once the interfaces that are associated with the MLP bundle are up, remove and reattach the service policy to the MLP bundle. If links associated with the bundle flap, the policy may have to be removed and reattached again.

- CSCed90846

  Symptoms: A class that contains the **priority percent** *percent* command and that is loaded at or greater than the specified rate leaves other classes with less than their fair bandwidth and adversely affects their bandwidth ratio.

  Conditions: This symptom is observed on Cisco 10000 series network interfaces at or above OC-3 speed.

  Workaround: There is no workaround.

- CSCed91338

  Symptoms: An ATM device that is connected to a Cisco 12000 series may cause a communication failure because of a length mismatch between the ATM adaption layer 5 (AAL5) and the IP data length.

Conditions: This symptom is observed when an IP frame that is smaller than 46 bytes in length comes from an Ethernet interface to an interface of an ATM line card (4OC3/ATM-IR-SC) on a Cisco 12000 series. The router always sets the length in the AAL5 to 54 bytes, as if the IP length is 46 bytes (which is the minimum length of the IP data plus an AAL5 header of 8 bytes).

Workaround: There is no workaround.

- CSCed91389

  Symptoms: OAMs are dropped on a Cisco router's ATM IMA interface that is configured for AAL5oMPLs, causing directly connected CE routers that have the **oam pvc-manage** command enabled to take the PVC down. As a result, the CE routers cannot forward any traffic to the MPLS core, thereby impacting basic connectivity between CE routers that are interconnected via the MPLS core. Errors are also see when the debug atm error command is enabled.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(28)S and that is configured for AAL5oMPLS on an ATM-IMA interface.

  Workaround: There is no workaround.

- CSCed91988

  Symptoms: The "Transmitted packets" column in the output of the **show policy interface** command for a particular interface may not be updated for packets that exit via this interface without being random or tail-dropped by WRED.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.2 S and that has WRED configured in an output service policy on an interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed92733

  Symptoms: On a Cisco 10720 router, when the system limit for the number of interfaces is surpassed, a software traceback is generated, indicating that a VCCI was not allocated. This traceback does not identify which interface caused the resource failure.

  Conditions: The problem is seen when the system limit on interfaces is reached. The most common scenario on a Cisco 10720 router is when the maximum number of VLANs is surpassed.

  Workaround: There is no workaround.

  Further Problem Description: The interface for which a VCCI is not allocated is not functional in PXF. The fix for this problem identifies that a resource allocation has failed and identifies which interface is affected.

- CSCed92837

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the standby Route Switch Processor (RSP) my hang just before downloading the image. This situation may prevent the router from entering the STANDBY-HOT state and from being capable to perform a switchover until the standby RSP is reset.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0 S or 12.2 S and that is configured for SSO/Nonstop Forwarding (NSF).

  Workaround: There is no workaround. After the problem occurs, you can recover the router by either waiting for an IPC timer to expire (the default time is 30 minutes) or by entering the **hw-module sec-cpu reset** command.

- CSCed93139

  Symptoms: Local and remote attachment circuit "Up events" may be ignored.

Conditions: This symptom is observed after a pseudowire virtual circuit is established.

Workaround: There is no workaround.

- CSCed94042

  Symptoms: A transient error may occur on a Cisco 12000 series line card during a network routing change. here is a chance that other line cards in the system will stop transmitting or receiving routing protocol updates and traffic, causing traffic to be blackholed.

  Conditions: This symptom is observed in an MPLS-VPN network. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb58214. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Enter the **microcode reload** command on any line card that stops receiving traffic or routing protocol adjacencies from its neighbors.

- CSCee00516

  Symptoms: An echo reply source address may be set incorrectly as 0.0.0.0 when responding to an echo request received on an unnumbered interface. Some line cards may check for the 0.0.0.0 source address condition and discard the packet based on that condition.

  Conditions: This symptom is observed during an LSP ping/traceroute. The symptom is platform independent.

  Workaround: Avoid using numbered interfaces. If this is not an option, there is no workaround.

- CSCee01223

  Symptoms: An external trigger may not cause a switchover from a working to a protect line card. The Rx K1/K2 values in the output of the **show aps** command are always 0x00/0x00.

  Conditions: This symptom is observed when two Cisco 10000 series routers are configured for MR-APS, with one router containing the working/active line card and the other router containing the protect/inactive line card. If the ADM that connects the working and the protect line cards initiates "FORCE/MANUAL" switchover, the active line card does not switch over to the protect line card.

  Workaround: There is no workaround.

- CSCee01698

  Symptoms: An Engine 4+ line card may corrupt MPLS packets, causing the packets to be dropped by the ingress line card of the next-hop router.

  Conditions: This occurs only with MPLS traffic. IP traffic works fine.

  Workaround: There is no workaround.

- CSCee02510

  Symptoms: High CPU utilization may occur on a Cisco 12000 series line cards due to the CEF scanner process.

  Conditions: This problem is seen when a large number of VPN routes are present on the router.

  Workaround: There is no workaround. However, the symptom does not seem to affect the convergence time or performance of the router.

- CSCee02683

  Symptoms: When you run Field Diagnostics and the router attempts to access the file through the LCI infrastructure, the entire router locks up. No commands or CLI responses are possible.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S.

Workaround: There is no workaround. To restore the router to normal operation, power-cycle the router.

- CSCee05224

  Symptoms: When you flap an interface that is attached to a L2TPv3 tunnel by entering the **shutdown** command followed by the **no shutdown** command or by causing the line protocol to enter the "DOWN/UP" mode, the tunnel enters the "SHUT" mode.

  Conditions: This symptom is observed on a Cisco 10720 router when the interface has the **xconnect** command enabled.

  Workaround: Disable and reenter the **xconnect** command on the affected interface.

- CSCee05882

  Symptoms: The queue size may not be set up correctly after a Cisco 10000

  Conditions: This symptom is observed when an MLP bundle has an output policy attached to an interface and the service policy contains WRED parameters.

  Workaround: Remove and reattach the service policy to the MLP bundle interface after the router has reloaded.

- CSCee06228

  Symptoms: The SRP protocol on a Cisco uBR7246VXR may not fully initialize during the boot sequence.

  Conditions: This symptom is observed on a Cisco uBR7246VXR running Cisco IOS Release 12.2(15)BC1b when one SRP side is wrapped. The symptom may also occur on a Cisco 7200 series and is not release-specific.

  Workaround: Force a wrap by entering the **srp ips request forced-switch** command and remove this forced wrap. Note that you have to do this manually after a reload/reboot.

- CSCee06794

  Symptoms: DTS may not work properly on dot1q Fast Ethernet subinterfaces. Traffic is not shaped at the expected rate

  Conditions: This problem is observed on a Cisco 7500 series that is configured as a PE router and that runs Cisco IOS Release 12.2(12i). The symptom may also occur in other releases.

  Workaround: If this is an option, use ISL subinterfaces.

- CSCee07446

  Symptoms: The **ping mpls pseudowire** and the **trace mpls pseudowire** commands may fail on a Cisco 12000 series.

  Conditions: This symptom is observed when you enter these commands for an Engine 3 line card.

  Workaround: There is no workaround.

- CSCee12235

  Symptoms: A Cisco platform reloads because of a watchdog timer expiration.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(20)S2 or Release 12.3 under the following conditions:

  - A service policy ("A") is attached to an ATM PVC.
  - Policy-map "A" is renamed to "B".
  - Service policy "B" is attached to the ATM PVC.

  Workaround: First detach the service policy from the PVC, then rename it and attach it again.

- CSCee12772

  Symptoms: On certain platforms (in particular but not limited to a Cisco 800 series), the CNS agents code that captures output for later transmission can crash.

  Conditions: This symptom is observed on a router that has configuration and EXEC agents and CNS agents that execute CLI commands when you send an XML file to direct these agents to execute a CLI command and return the output (if there is any output).

  Workaround: Telnet into the router (not through the console) and exit. This may need to be done multiple times.

- CSCee13315

  Symptoms: A router crashes when you attach a policy map to an interface.

  Conditions: This symptom is observed when you remove random detect from a class, remove a class that has random detect configured, or remove a policy map with a class that has random detect configured.

  Workaround: There is no workaround.

- CSCee16581

  Symptoms: Traffic is sent using the “net ctrl” queue on the egress interface.

  Conditions: This problem occurs on a Cisco 10720 router when IPv6 high-priority traffic (110 or 111 in the first 3 bits of the IPv6 traffic class) is forwarded.

  Workaround: There is no workaround.

- CSCee16950

  Symptoms: IPv6 traffic forwarding on an Engine 2 DPT line card is performed by the CPU of the line card; IS-IS, OSPFv2 or OSPFv3 adjacencies, or BGP neighbourships across any of the interfaces of the Engine 2 DPT line card may fail.

  Conditions: This symptom is observed when oversubscribing the CPU of the Engine 2 DPT line card in terms of its maximum IPv6 packet-per-second forwarding rate, which is about 100 Kpps.

  Workaround: There is no workaround. The symptom does not occur for POS and GE Engine 2 line cards.

- CSCee18844

  Symptoms: Traffic forwarding problems may occur when sending MVPN traffic from multiple sources to the same group.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as an MVPN decapsulation PE router with an Engine 3 line card that forwards multicast packets on an VRF interface.

  Workaround: To ensure that no collisions occur on the VRF interface, configure hardware multicast on the Engine 3 line card by entering the **hw-module slot** *number* **ip multicast hw-accelerate source-table size** *x* **offset** *y* command.

- CSCee19222

  Symptoms: An MLP bundle configured between a Cisco 7500 series and any other router may not be able to switch traffic when dCEF is enabled on the Cisco 7500 series.

  Conditions: This symptom is observed when LFI is enabled with one member link in the MLP bundle.

Workaround: Either remove dCEF or remove LFI. (A combination of CEF and MLP is not supported.) Note that if there are two member links in the interleaving-enabled MLP bundle, the problem does not occur.

- CSCee24263

  Symptoms: A PVC may be inactive and may not come up.

  Conditions: This symptom is observed when a VC is deleted or removed and you try to recreate the same VC.

  Workaround: Save the configuration and reload the router.

- CSCee30549

  Symptoms: Some interfaces on a channelized SONET line card may not carry bidirectional traffic following an APS switchover. Interfaces may be up and routes may be present when this occurs.

  Conditions: The symptom is only observed on a Cisco 12000 series 1-port OC-12 line card (channelized to DS1) that functions in an 1+1 APS configuration. The symptom could occur on any channelized APS interface.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

- CSCee35349

  Symptoms: When you set up an L2TPv3 tunnel configured in the PW class, a ping cannot go through from CE router 1 to CE router 2 until the ping is initiated by CE router 2.

  Conditions: This failure occurs in Cisco IOS Release 12.0(28)S with a Fast Ethernet interface (not with a serial or POS interface).

  Workaround: First, ping from CE router 2 to CE router 1. Then, ping from CE router 1 to CE router 2.

- CSCee36744

  Symptoms: An RP may crash when you add or remove a channel group to or from a 4-port ISE Gigabit Ethernet line card or when you reload microcode onto the line card on which channel group members are configured.

  Conditions: This symptom observed on a Cisco 12000 series when there are link-bundle subinterfaces configured on the 4-port ISE Gigabit Ethernet line card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed63480. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: There is no workaround.

- CSCee40938

  Symptoms: FRoMPLS traffic fails with an Engine 3 line card as the disposition card.

  Conditions: This symptom is observed with any DLCI (xx xxxx xx11) that uses the two LSBs in its “ckt” ID. This problem is seen because of the corruption of the two LSBs during a disposition update.

  Workaround: There is no workaround.

- CSCee42281

  Symptoms: Some interfaces on a channelized SONET line card may not carry bidirectional traffic following an APS switchover. Interfaces may be up and routes may be present when this occurs.

Conditions: The symptom is observed on Cisco 12000 series Engine 3 channelized line cards (OC-48 or 4XOC-12 channelized to DS-3) that functions in an 1+1 APS configuration. However the symptom could occur on any channelized APS interface.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

- CSCin33783

  Symptoms: Entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an Gigabit Ethernet interface may prevent customer edge-to-customer edge (CE-to-CE) pings from going through.

  Conditions: This symptom is observed when Ethernet over Multiprotocol Label Switching (EoMPLS) is configured in VLAN mode on the Gigabit Ethernet interface of a Network Processing Engine G1 (NPE-G1) on a Cisco 7200 series.

  Workaround: Configure EoMPLS in VLAN mode on a port adapter such as a Gigabit Ethernet or Fast Ethernet port adapter.

- CSCin41269

  Symptoms: A controller of an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) may fail to come up after the router has booted up.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-8TE1+. The symptom is platform independent and port adapter dependent.

  Workaround: Enter the **shutdown** controller configuration command followed the **no shutdown** controller configuration command on the affected controller.

  Alternate Workaround: Enter the **clear counters** user EXEC or privileged EXEC command on the affected interface of the PA-MC-8TE1+.

- CSCin52138

  Symptoms: When flaps occur on an Inverse Multiplexing over ATM (IMA) group interface on which the Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: VC Mode feature is configured, input packets may be switched via Cisco Express Forwarding (CEF).

  Conditions: This symptom is observed on a Cisco 7500 series that has an IMA group interface that is configured on a Versatile Interface Processor (VIP).

  Workaround: Perform an online insertion and removal (OIR) of the VIP.

- CSCin61140

  Symptoms: A line card reloads continuously after an OIR.

  Conditions: This symptom is observed when the line card has MFR and a service policy configured.

  Workaround: Remove the service policy before performing an OIR.

- CSCin62978

  Symptoms: A FlexWAN, enhanced FlexWAN, or Versatile Interface Processor that has a PA-MC-E3 or PA-MC-T3 installed may crash.

  Conditions: This symptom is observed under rare conditions in a stress situation with dFLI and dCRTP configured.

  Workaround: There is no workaround.

- CSCin64927

  Symptoms: The **xconnect** command is not supported on Q-in-Q subinterfaces but the command-line interface (CLI) parser does not prevent you from configuring this command on Q-in-Q subinterfaces.

  Conditions: This symptom is observed on platforms other than the Cisco 12000 series.

  Workaround: There is no workaround.

- CSCin66535

  Symptoms: On a Cisco 7500 series router, after a RPR, RPR-plus or SSO switchover, the router may display the following message:

  ```
  %RSP-3-RESTART: cbus complex
  ```

  This will be followed by the reload of all VIPS in the router and the following message:

  ```
  HA-2-NO_QUIESCE: Slot <slot#> did not quiesce, it will be disabled and then reloaded.
  ```

  Conditions: This problem happens on a Cisco 7500 series router that is running Cisco IOS Release 12.0 S and occurs after an RPR, RPR-plus, or SSO switchover. Similar symptoms can be observed if the **service single-slot-reload-enable** command is not configured on the router, but in this case, the cbus complex message will follow the "HA-2-NO_QUIESCE" error message.

  Workaround: There is no workaround.

- CSCin66542

  Symptoms: The line protocol on a T1 of a T3 controller in a PA-MC-2T3+ port adapter may stay in the down state even when looped.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series.

  Workaround: There is no workaround.

- CSCin70454

  Symptoms: A PPP session may stay down after a long series of link flaps.

  Conditions: This symptom is observed when MLP/LFI is enabled on an ATM PVC.

  Workaround: There is no workaround.

- CSCin72219

  Symptoms: If you enter the **shutdown** command followed by the **no shutdown** command on an interface, traffic that congests the interface may cause the router to crash.

  Conditions: This symptom is observed when a policy is attached to the interface.

  Workaround: There is no workaround.

- CSCin73703

  Symptoms: A router may crash when you enter the **set fr-fecn-becn** command.

  Conditions: This symptom is observed when you enter the **set fr-fecn-becn** command for an unsupported interface (that is, a non-Frame Relay interface).

  Workaround: There is no workaround.

- CSCuk48013

  Symptoms: A Cisco 7500 series router that is running 12.0S may drop traffic to a static route after a microcode reload. The symptom may also occur in other releases.

  Conditions: Traffic loss will occur for static routes to /32 prefixes that are attached to an interface, that is, the **ip route** *prefix mask interface-type interface-number* command is enabled.

Workaround: Disable Cisco Express Forwarding (CEF) by entering the **no ip cef** command. Then, reenable CEF by entering the **ip cef distributed** command.

- CSCuk48156

  Symptoms: Failover boot commands from a slot to a disk results in an endless loop. If the router does not find the image in slot0, it will not be able to properly switch to the next image in disk1.

  Conditions: This symptom occurs when slot0 holds a linear flash card and disk1 holds an ATA disk.

  Workaround: While being in a loop on the console connection, press control plus return, type, and send a break until the loop stops.

- CSCuk48189

  Symptoms: Changing a policy map while it is applied to several subinterfaces may cause traffic to stop flowing or may prevent QoS features from functioning correctly.

  Conditions: This symptom is observed on a Cisco 12000 ATM ISE line card.

  Workaround: There is no workaround.

- CSCuk48191

  Symptoms: An input policy map containing the **shape** command without the **police** command does not function properly when it is applied to an interface that has a rate limit enabled.

  Conditions: This symptom is observed on a Cisco 12000 ATM ISE line card.

  Workaround: There is no workaround.

- CSCuk48314

  Symptoms: During an SSO switchover, the newly active Route Processor (RP) may output the following error message:

  ```
  %SCHED-7-WATCH: Attempt to monitor uninitialized watched queue (address 0).
  -Process= "CEF LC IPC Background"
  ```

  This error is harmless, and no functional problem will occur when this error is received.

  Conditions: This symptom occurs during an SSO switchover.

  Workaround: There is no workaround.

- CSCuk48808

  Symptoms: Following an OIR, the **show ip cef inconsistency now** command may report an inconsistency between an RP and a VIP. There are no inconsistencies reported on the VIP itself.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0 S.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCeb21552

  Symptoms: The following error message may be displayed when a router receives a connection request on command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports:

  ```
  %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.2.2
  ```

  Conditions: This symptom is observed on a Cisco router that has the remote shell (rsh) disabled.

  Workaround: Filter the traffic that is destined for command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports.

First, enter the **show ip interface brief** EXEC command to display the usability status of interfaces that are configured for IP. The output may look like the following:

```
Interface      IP-Address      OK? Method Status                Protocol
Ethernet0/0    172.16.1.1      YES NVRAM  up                    up
Ethernet1/0    unassigned      YES NVRAM  administratively down down
Serial2/0      192.168.2.1     YES NVRAM  up                    up
Serial3/0      192.168.3.1     YES NVRAM  up                    up
Loopback0      10.1.1.1        YES NVRAM  up                    up
```

Then, create the following access control list (ACL) for the router and apply this ACL to all interfaces that are enabled with the **ip access-group 177 in** router configuration command:

```
access-list 177 deny tcp any host 172.16.1.1 eq 514
access-list 177 deny tcp any host 172.16.1.1 eq 544
access-list 177 deny tcp any host 192.168.2.1 eq 514
access-list 177 deny tcp any host 192.168.2.1 eq 544
access-list 177 deny tcp any host 192.168.3.1 eq 514
access-list 177 deny tcp any host 192.168.3.1 eq 544
access-list 177 deny tcp any host 10.1.1.1 eq 514
access-list 177 deny tcp any host 10.1.1.1 eq 544
access-list 177 permit ip any any
```

- CSCed21865

  Symptoms: A router may reload unexpectedly when a TCP watchdog timer expires.

  Conditions: This symptom is observed when the router has hundreds of Border Gateway Protocol (BGP) peers.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCea63481

  Symptoms: A Cisco router may reboot every five minutes, and the system may return to ROM because of a bus error at PC 0x400F047C, address 0x630BC42E.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp- jsv-mz image of Cisco IOS Release 12.2(15)T. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCec83030

  Symptoms: A parity error on a Versatile Interface Processor (VIP) card may cause other VIPs to go to a wedged state.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCed02028

  Symptoms: A router may reload unexpectedly because of a bus error after the following error message is displayed:

  ```
  %ATMPA-3-BADVCD:ATM[int] bad vcd [number] packet -
  ```

  Conditions: This symptom is observed on a Cisco router that is configured with an ATM interface.

Conditions: This symptom is observed on a Cisco router that is configured with an ATM interface when a packet that contains a virtual circuit descriptor (VCD) that is out range is passed on to the ATM driver of the interface in order to be transmitted.

Workaround: There is no workaround.

- CSCed29275

  Symptoms: IP VRF interfaces that are configured Frame Relay may not work. That is, locally generated and forwarded packets that are received on these interfaces may not be processed correctly.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the Frame Relay subinterfaces that have a VRF configured.

- CSCed40110

  Symptoms: When a router running Cisco IOS Release 12.0S, 12.1, 12.2, or 12.2T receives a multilink packet with Protocol Field Compression (PFC) applied, the packet is not interpreted correctly, and is subsequently rejected. The following debug messages appear in the debug trace when the **debug ppp negotiation** command is enabled:

  ```
  MLP: I UNKNOWN(192) [Not negotiated] id 0 len 0
  LCP: O PROTREJ [Open] id 2 len 95 protocol MLP
  ```

  Conditions: This symptom is observed when the router requests PFC during Link Control Protocol (LCP) negotiations and the peer applies PFC to its outbound packets. PFC is enabled by default on asynchronous serial interfaces, it is disabled by default on other interfaces.

  Workaround: In Cisco IOS Release 12.2 and 12.2T, PFC can be disabled using the **ppp pfc local forbid** interface configuration command. In Release 12.0S and 12.1, there is no workaround.

- CSCed52817

  Symptoms: Even though you remove the **frame-relay fragment** command from an active RP, the command may be back in the configuration after a switchover.

  Conditions: This symptom is observed on a Cisco 10000 series, but not on a Cisco 7500 series and Cisco 12000 series.

  Workaround: After you have removed the **frame-relay fragment**, **frame-relay interface-queue**, or **frame-relay ip rtp** command from a map class on the active RP, reset the standby RP to enable the standby RP to read the configuration changes.

- CSCed59264

  Symptoms: L3 broadcasts such as EIGRP are not transmitted on Frame Relay PVC bundles.

  Conditions: This symptom is observed when EIGRP or OSPF is unable to set up routes that are learnt via an interface that has a Frame Relay PVC bundle configured.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(27)S5

Cisco IOS Release 12.0(27)S5 is a rebuild of Cisco IOS Release 12.0(27)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(27)S5 but may be open in previous Cisco IOS releases. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCee83917

  Symptoms: The RP of a Cisco router may crash when entering the **write memory** legacy command.

  Conditions: This symptom is observed on a Cisco router that has the **snmp mib community-map** command enabled with a very long community string and an engineID. The symptom may also occur when the long community string is removed from the configuration. The symptom does not occur when entering the **copy running-config startup-config** EXEC command.

  Workaround: A community string that is shorter than 40 characters will not cause the symptom to occur.

- CSCeg16078

  Symptoms: You cannot create a VRF-aware ICMP, UDP, or jitter probe using SNMP.

  Symptoms: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(27)S. Note that the symptom does not occur in Release 12.2(11)T.

  Workaround: Use CLI commands to create a probe.

- CSCeg23428

  Symptoms: After you perform an OIR of a VIP, reload microcode onto a VIP, or after a VIP crashes, an MLP or MFR interface that is shut down comes up unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series only with virtual interfaces and only the first time that you perform an OIR or reload microcode or that the VIP crashes after the router has booted up. The symptom does not occur when you perform subsequent OIRs or reload microcode again or when the VIP crashes again.

  Workaround: There is no workaround.

- CSCeh47604

  Symptoms: An OER border component does not sent passive updates for OER prefixes, preventing the prefixes from being controlled. The prefixes cycle from the default state to the hold-down state back to the default state.

  Conditions: This symptom is observed when NetFlow is configured and when the mode monitor is configured to be "passive" or "both".

  Workaround: Configure the mode monitor to be "active". The functionality of the mode monitor is limited to the "active" mode only.

IP Routing Protocols

- CSCdr31946

  Symptoms: A Cisco router that is runs Enhanced Interior Gateway Routing Protocol (EIGRP) with the stub feature enabled may have a route that is active and not waiting for replies.

Conditions: This symptom is observed only in networks where all of the EIGRP neighbors are declared as stub.

Workaround: Remove the EIGRP stub feature or clear the IP EIGRP neighbors.

- CSCea59206

  Symptoms: When you configure the **distribute-list** router configuration command under the **address-family ipv4 vrf** *vrf name* router configuration command, the **distribute-list** router configuration command may appear under the main routing process as may be displayed in the output of the **show running-config** EXEC command.

  Conditions: This symptom is observed in either a Routing Information Protocol version 2 (RIPv2) or a Border Gateway Protocol (BGP) configuration when you specify the *interface-type* and *interface-number* arguments of the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} [*interface-type interface-number*] router configuration command.

  The symptom does not occur when you do not define the *interface-type* and *interface-number* arguments and only enter the **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**} router configuration command.

  Workaround: There is no workaround.

- CSCed33044

  Symptoms: ARP may not function properly on the remote side of point-to-point Fast Ethernet link with a default static route until the remote side is pinged.

  Conditions: This symptom is observed on a Cisco router when ARP and /31 mask are configured on a point-to-point link Fast Ethernet link with a default static route. The symptom is platform-independent.

  Workaround: There are four different workarounds:

  - Use a /30 netmask on the point-to-point Fast Ethernet connection.

  - Configure a static ARP entry for the remote side of the Fast Ethernet link.

  - Enter the **ip proxy-arp** command on the remote side of the Fast Ethernet link.

  - Use an OSPF route instead of a default static route.

- CSCee11274

  Symptoms: BGP may fail to reestablish a session when you remove a line card, PA, VIP, or module and replace it with a card of a different type. For example, the problem occurs when you remove a 1-port GE line card and replace it with a 3-port GE line card. However, if you replace the 1-port GE line card with another 1-port GE line card (or you just plug the same 1-port GE line card back in the chassis), the problem does not occur.

  Conditions: This symptom is observed when the router one side of the BGP session is configured with the **neighbor** *ip-address* **transport connection-mode active** command and when a line card, PA, VIP, or module is changed on the router at the other side of the BGP session. Furthermore, the router at the other side of the BGP session is configured with the **neighbor** *ip-address* **update-source** *interface* command, and the *interface* argument refers to the interface on the line card, PA, VIP, or module that is changed.

  Workaround: Disable and reenter the **neighbor** *ip-address* **update-source** command.

- CSCee88542

  Symptoms: A Cisco router may reload unexpectedly when you enter the **show ip msdp peer** command.

Conditions: This symptom is observed when the MSDP session flaps while you enter the **show ip msdp peer** command.

Workaround: There is no workaround.

- CSCef57803

  Symptoms: In a VPNv4 network in which a multi-homed CE router advertises multiple paths for a prefix, a PE router may fail to withdraw the prefix previously advertised to another PE router when its best path changes from a non-imported path to an imported path because of a change in the import route map of the VRF.

  Conditions: This symptom is observed in a topology in which a CE router connects to a PE router via two different VRFs.

  Workaround: Remove the imported path either by unconfiguring the import route map of the VRF or by changing the import route target, withdraw the non-imported prefix from the CE router, and restore the import route map or import route target.

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don’t Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef93215

  Symptoms: A router that is configured for OSPF may reload unexpectedly and reference the "ospf_build_one_paced_update" process.

  Conditions: This is observed on a Cisco router that has a mixture of LSAs (of type 5 and 11) that travel throughout an autonomous system and LSAs (of any type other than type 5 and 11) that travel within a particular OSPF area. The symptom may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA.

  Workaround: There is no workaround.

Further Problem Description: The symptom is very unlikely to occur. The symptom does not occur on a router that has exclusively stub areas and NSSA areas. The symptom may occur when a router does not have exclusively stub areas and NSSA areas.

- CSCeg30291

  Symptoms: BGP fails to send an update or withdraw message to some peers when these peers have failed to converge properly after an earlier attempt.

  Conditions: This symptom is observed on a Cisco router when you enter the **clear ip bgp** *neighbor-address* **soft out** command while BGP is in the middle of converging. The symptom does not occur when network traffic load is low and BGP has converged.

  Workaround: To clear the error condition, enter the **clear ip bgp** *neighbor-address* **soft out** command again. Alternately, enter the **clear ip bgp** *neighbor-address* command (that is, without the **soft out** keyword).

- CSCeg54375

  Symptoms: Routing inconsistencies may occur in the RIB: routes may be missing from the RIB but may be present in the BGP table.

  Conditions: This symptom is observed on a Cisco RPM-XF when the toaster processor crashes. However, the symptom may occur on any platform that has a toaster processor.

  Workaround: Enter the **clear ip route vrf** *vrf-name* ***** command.

- CSCeg70726

  Symptoms: A router may crash when you enable MVPN by entering the **mdt default** *group-address* command under a VRF.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

  Workaround: There is no workaround.

- CSCeh16989

  Symptoms: The Multiprotocol BGP (MP-BGP) network entries counter increases above the real number of reachable networks.

  Conditions: This symptom is observed when network activity occurs in a non-converged environment. The correct number of network entries is restored when there is a period of BGP stability that last for about 1 minute or more because BGP is able to converge and the scanner has time to run and collect the old network entries. However, if there is a sustained period of churn and BGP is only able to converge for a few seconds before new updates arrive, old BGP network entries are not cleaned up, causing the MP-BGP network entries counter to increase above the real number of reachable networks.

  Workaround: There is no workaround.

- CSCuk54787

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb68673

  Symptoms: On an ASBR-PE, the TFIB may be missing a forwarding entry for a prefix that is learnt from a PE.

  Conditions: This symptom is observed on an "ABSR-co-located PE" (that is, an ASBR that also functions as a PE router) when the PE functionality is removed by deconfiguring VRF, for example, by entering the **no ip vrf** *vrf-name* command.

  Since this is a timing issue, it may occur in Cisco IOS Release 12.0 S, Release 12.2 S, Release 12.2 T, and Release 12.3.

  Workaround: There is no workaround.

- CSCeb84128

  Symptoms: A Cisco 10000 series may stop responding.

  Conditions: This symptom is observed when you attach a child policy map with four policing statements to a parent policy map with a bandwidth queue and when the parent policy map is already attached to 100 T1 interfaces.

  Workaround: Attach the child policy map to the parent policy map before you attach the parent policy map to the interfaces.

- CSCec25942

  Symptoms: A POS Engine 2 line card originates a high traffic volume to a downstream router over a POS link because the same packet is sent over and over.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(22)S5.

  Workaround: There is no workaround.

- CSCed16284

  Symptoms: Packet precedence on rate-limit actions with transmit is incorrectly remaining the same because the **set-prec- transmit** action is not working.

  Conditions: The interface configuration includes rate limiting with actions that sets precedence to change on conform and/or exceed with the **rate-limit** command that includes **conform-action set-prec-transmit 1** and **exceed-action set-prec-transmit 0**. The packets received are initially at Precedence of 2, but instead of changing to either a Precedence of 1 or a Precedence of 0, all packets are transmitted still at a Precedence of 2. The numbers 0, 1, and 2 are examples and can be any number in the range of 0-7.

  Workaround: There is no workaround.

- CSCed89760

  Symptoms: When a primary CSC switchover happens on a Cisco 12800 series, a line card may reset.

  Conditions: This symptom is observed when there is primary CSC switchover, either through a CLI command or a physically removal of the primary CSC.

  Workaround: There is no workaround.

- CSCee04893

  Symptoms: A Cisco router is not able to forward traffic to a TE tunnel.

  Conditions: This symptom has been observed on a Cisco 10000 running Cisco IOS Release 12.0(26)S1 and Release 12.0(27.3)S1 with Multilink PPP + MPLS + TE Tunnel.

Workaround: There is no workaround.

- CSCee18679

  Symptoms: When you use snmpget to retrieve information directly from the ifIndex table, the following error message is generated:

  ```
  No Such Instance currently exists at this OID.
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S.

  Workaround: Do not snmpget. Rather, use snmpwalk or snmpgetnext.

- CSCee43259

  Symptoms: In the case of a Cisco 12000 series router using Supervisor Engine 3 ISE QOC12 ATM card, Route Processor (RP) may hang for about 15-20 minutes and crash when the following two steps are done:

  Conditions: * Configure 1K ATM PVCs (1K ATM sub-interfaces) with a class-default (queue- limit) based service-policy configured on all of the PVCs (service-policy should be configured under each PVC to see RP hangs and crash).

  * On removing the above 1k ATM PVCs (sub-interfaces), RP hangs for about 15-20 minutes before the user can regain control.

  The following warning message may show up when deleting the ATM sub-intfs:

  %WARNING: Features on ATM6/0.1 haven't been removed Please wait for approximately ten minutes and retry. % Removal of physical interfaces is not permitted.

  * On adding the 1K sub-intfs again (second attempt), RP crashes. This RP crash is reproducible.

  Workaround: There is no workaround.

- CSCee49035

  Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

  Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

  Workaround: There is no workaround.

- CSCee66058

  Symptoms: SNMP users that have MD5 configured may become lost after a switchover in an RPR+ environment.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series that run Cisco IOS Release 12.0(27)S1 in RPR+ mode.

  Workaround: There is no workaround.

- CSCee81490

  Symptoms: MALLOCFAIL messages may be generated during an attempt to allocate large negative and positive memory blocks in the "cpf_process_ipcQ" process:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of -1622998781 bytes failed from
  0x60B5BE48, alignment 0
  Pool: Processor  Free: 371055532  Cause: Not enough free memory
  Alternate Pool: None Free: 0  Cause: No Alternate pool
  ```

```
-Process= "cpf_process_ipcQ", ipl= 0, pid= 141
-Traceback= 603DDCB0 603E005C 60B5BE50 60B5C140 60B5C62C 60B59A0C 603D5D1C
603D5D08

%SYS-2-MALLOCFAIL: Memory allocation of 344820739 bytes failed from
0x60B5BE48, alignment 0
Pool: Processor  Free: 363937412  Cause: Memory fragmentation
Alternate Pool: None Free: 0  Cause: No Alternate pool
-Process= "cpf_process_ipcQ", ipl= 0, pid= 141
-Traceback= 603DDCB0 603E005C 60B5BE50 60B5C140 60B5C62C 60B59A0C 603D5D1C
603D5D08
```

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(24)S5.

Workaround: There is no workaround.

- CSCef06848

  Symptoms: Packets are not load-balanced between interfaces of different POS line cards or POS port adapters.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(25)S or Release 12.0(26)S2 and that has two BGP peers. Four static routes are configured on interfaces of one POS line card or POS port adapter to the loopback IP address of one BGP peer and another four static routes are configured on interfaces of another POS line card or POS port adapter to the loopback IP address of the other BGP peer.

  In this configuration, 85 percent of the traffic runs via the output interfaces on one POS line card or POS port adapter. When you enter the The **clear adjacency** command, 85 percent of the traffic runs via the output interfaces on the other POS line card or POS port adapter.

  Workaround: There is no workaround.

- CSCef20602

  Symptoms: A static route to a default route that points at a non-directly connected next hop (a recursive route) may not be properly downloaded to the hardware CEF entry on an Engine 6 line card.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: Configure the default route to point to a directly-connected next hop.

- CSCef23912

  Symptoms: A traceback is generated on the console and logged in the logging buffer, and the count in the output of the **show alignment** command increments.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured as a provider edge (PE) router when you enter the **show mpls forwarding** command to show the pop labels and the active LDP peers.

  Workaround: There is no workaround.

- CSCef25686

  Symptoms: A number of PVCs may become locked in an inactive state, and the following type of error message may appear in the log:

  ```
  %ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=X, VPI=X, VCI=X) on Interface
  ATM X/X/X,
  ```

```
(Cause of the failure: PVC removal during recreation failed)
```

Conditions: This symptom is observed when you change the parameters of a VC class while the PVC is active and while you view the PVC status in the output of the **show atm vc interface** *interface-number* command.

The symptom occurs when you change the PVC speed in a VC class via one Telnet (or console) session and you enter the **show atm vc interface** *interface-number* command via another Telnet (or console) session.

Workaround: To remotely resolve the symptoms, remotely initiate an HA failover or remotely reload the affected router.

- CSCef26053

  Symptoms: Load-balancing does not work over a BGP multipath. Some of the traffic may be forwarded correctly while other traffic may be forwarded unlabeled into the MPLS core.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the following conditions are present:

  - The affected route is in a VRF.

  - One of the paths is learned from a CE router via an eBGP multihop session.

  - The eBGP multihop peer (that is, the CE router) is reachable through the MPLS core and the BGP session does not involve a label exchange.

  Workaround: Avoid a multihop eBGP session in which the CE router is reachable through the MPLS core. For example, instead of a configuration in which the CE router connects to the PE router across the MPLS core, configure the CE peer to connect to a local PE router that redistributes the routes it has learned from the CE peer to other PE routers. (The local PE router may need to be configured for eiBGP multipath.)

- CSCef43691

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don’t Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef53109

  Symptoms: When you enter the **do** command with arguments on an interface member of a port-channel or pos-channel group, a message sinmilar to the following one is displayed:

  ```
  Command "do <arguments>" not allowed on link-bundle member interface
  <interface-number>
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S when the command is entered on an interface member of a port-channel or pos-channel group.

  Workaround: Enter the command directly on the interface that you are querying.

- CSCef53475

  Symptoms: Packet drops occur when traffic is sent below the shape rate that is defined in a service policy.

  Conditions: This symptom is observed on a Frame Relay interface when there are multiple DLCIs that have service policies enabled. Each DLCI has a hierarchical policy with a shape rate in the class default at the parent level and a child policy with LLQ and CBWFQ classes. When traffic to each DLCI is just below the shape rate and the combined traffic through the interface is close to line rate, packet drops occur on some DLCIs. The symptom does not occur when traffic is sent to one DLCI at the time.

  Workaround: Increase the shape rate to compensate for the scheduling inaccuracy.

- CSCef59507

  Symptoms: A failed LDP session may still show up in the output of the **show mpls ldp neighbors** command as well as the new working session after the neighborship is re-established. The display of two sessions, one not working and one working to the same neighbor, may mislead the MPLS network operator.

  Conditions: This symptom may occur after an LDP session has gone down and then re-established.

  Workaround: There is no workaround.

- CSCef61610

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages

  2. Attacks that use ICMP "fragmentation needed and Don’t Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef63272

  Symptoms: A recursive static default route may not have an outgoing MPLS label, causing all packets to be dropped.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(9) but may also occur in other releases.

  Workaround: Add a nonrecursive static route to the BGP next-hop.

- CSCef64744

  Symptoms: On a 6-port channelized T3 line card that is enabled for QoS, a low latency queue (LLQ) may not receive traffic that is mapped to the LLQ.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1.

  Workaround: Reload the line card. If this is not an option, there is no workaround.

- CSCef69631

  Symptoms: All line cards may reset and may not enter the "RUN" state after a software OIR or the primary CSC occurs on a Cisco 12000 series that has 40 GB of fabric.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of an interim release for Cisco IOS Release 12.0(30)S. However, this caveat is resolved in Release 12.0(30)S.

  Workaround: Power cycle the router.

- CSCef97190

  Symptoms: The "giants" counter increments continuously for a serial T1 interface when MR-APS is configured on a 4-port channelized STM-1 line card. The symptom occurs even when the fiber is pulled from the OC-3 port.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.3(7)XI1 when the serial T1 interface is in the inactive state, irrespective of whether it is the working interface or the protect interface. The symptom does not occur when the serial T1 interface is in the active state, again irrespective of whether it is the working interface or the protect interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg03606

  Symptoms: Multicast VPN (MVPN) traffic does not resume.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that functions as a PE router that is configured for MVPN.

  Workaround: Enter the **clear ip mroute** command.

- CSCeg05681

  Symptoms: A CSC OIR may cause all line cards in a router to enter the disabled state and the standby RP to reload continuously.

  Conditions: The symptom is observed on a Cisco 12000 series that has dual PRPs and that runs a Cisco IOS interim release for Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCeg12649

  Symptoms: On a Cisco router that functions as an egress PE router in an MPLS VPN network, after the customer-facing line card is reloaded, the ingress line card that receives an incoming VPN label with a destination with a glean adjacency (which requires an ARP request) without a BGP session may not properly complete the adjacency, causing traffic to be dropped.

  Conditions: This symptom is mostly observed with static recursive route configurations. You can recover from the symptom by manually pinging the interface of the CE router from the adjacent PE router.

  Workaround: Confure static ARP entries for the next hop router in the static recursive routes.

- CSCeg19635

  Symptoms: The PXF engine on a Cisco 10000 series may crash, causing traffic through the router to be interrupted temporarily.

  Conditions: This symptom is observed on a Cisco 10000 series when a security ACL is changed and immediately applied to an interface while traffic is traversing the interface. The symptom may occur on a Cisco 10000 series that is configured with either a PRE1 or a PRE2.

  Workaround: Wait several seconds between updating the ACL and applying it to the interface.

- CSCeg20771

  Symptoms: During intense interaction between the RP and line cards, the RP may crash because of a corruption. This symptom occurs when large numbers of VRFs are continuously created and deleted. However, the trigger for the symptom to occur could be caused by something else.

  Conditions: This symptom is observed on a Cisco 12410 that is configured with about 100 VRFs and that runs Cisco IOS Release 12.0(27)S2, 12.0(28)S1, or an interim release for Release 12.0(29)S. The symptom is not observed in Release 12.0(30)S.

  Workaround: Do not add or delete more than VRFs at one time.

- CSCeg25493

  Symptoms: Several VIPs may crash at about the same time because of a bus error.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S4 and that is configured with an RSP4 when the VIPs are configured for QoS but have insufficient memory.

  Workaround: Increase the amount of memory on the VIPs.

- CSCeg36748

  Symptoms: The **show redundancy** command incorrectly indicates Peer RP is disabled during the upgrade procedure when it is not.

  Conditions: This symptom is observed on a Cisco 12000 series router that runs the gsr-p-mz image of Cisco IOS Release 12.0(27)S and 12.0(28)S.

  Workaround: Continue with the upgrade procedure.

- CSCeg37524

  Symptoms: A 4-port OC-12 ATM single mode (4OC12/ATM-IR-SC) line card may generate unicast send timeout errors, %LC-3-PSAERRS errors, and %LC-3-BMAERRS errors, which cause TDP neighbor flapping and may cause the line card to crash.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3.

  Workaround: There is no workaround.

- CSCeg66282

  Symptoms: The controller of a 1-port multichannel STM-1 port adapter (PA-MC-STM1) does not come up after the router has reloaded.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(28)S2. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeg66627

  Symptoms: An Engine 6 line card may reset because of an IPC timeout and may generate the following error message:

  %MCC192-3-CPUIF_ERR: Packet Exceeds Programmed Length

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3.

  Workaround: There is no workaround.

- CSCeg73076

  Symptoms: A Cisco 10000 series reloads when a large QoS policy is defined.

  Conditions: The symptom is observed when you define a policy map that exceeds the number of classes that can be defined in a policy (32).

  Workaround: Avoid policies with an unsupported number of classes.

- CSCeg79456

  Symptoms: An Engine 6 line card may reset because of an IPC timeout.

  Conditions: This symptom is observed on a Cisco 12816 that runs Cisco IOS Release 12.0(27)S4 when you enter the **shutdown** command on the primary Clock Scheduler Card (CSC) or you enter the **no shutdown** command on the secondary CSC that is in the shut down state.

  Workaround: There is no workaround.

- CSCeg83399

  Symptoms: When an ATM PVC is configured with an egress service policy, exiting from the PVC configuration mode by entering the **exit** command may cause traffic that is forwarded from other PVCs on the line card to be dropped.

  Conditions: This symptom is observed on a Cisco 12000 series router that is configured with an ATM ISE line card or an 8-port OC-3 ATM Engine 2 line card.

  Any action that causes the affected ATM PVC to be reinitialized restores traffic forwarding.

  Workaround: Do not enter the **exit** command to exit from the PVC configuration mode. Rather, enter the **end** command.

- CSCeh00169

  Symptoms: After you have reloaded a router, for each of the service policies that are attached to the interfaces of a 4-port OC-12 POS ISE line card, the policing of L2 VCs may fail when errors with the following associated error messages occur:

  ```
  "Must remove existing service policy first .."
  ```

  or

  ```
  "Configured exceed actions are not supported when policing L2 VCs on interface.."
  When the policing of L2 VCs fails, the following error message is generated:
  "L2 policing config failed."
  ```

Conditions: This symptom is observed on a Cisco 12416 that runs the c12kprp-p-mz image of a Cisco IOS interim release for Release 12.0(31)S and that is configured with dual PRPs and 4-port OC-12 POS ISE line card that has a service policy attached to each of its interfaces.

Following are examples of configurations that may trigger the symptoms:

```
policy-map testing-input
 class class-default
  police cir percent 2 pir percent 4
   conform-action set-mpls-exp-imposition-transmit 4
   exceed-action set-mpls-exp-imposition-transmit 1
   violate-action drop
!
map-class frame-relay testing
 service-policy input testing-input

interface POS6/0
 frame-relay interface-dlci 17 switched
  class testing
```

Workaround: There is no workaround.

- CSCeh02579

  Symptoms: A multilink bundle on a Cisco 10000 series may lock up. The multilink bundle may transmit packets but does not process any incoming packets, indicating that all links of the bundle are in an out-of-order state and draining.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX, Release 12.0(26)S4, or a later 12.0S release and that is configured for mVPN and MLP. The symptom may be platform-independent.

  Workaround: If this is an option, disable mVPN.

- CSCeh07851

  Symptoms: There are several symptoms:

  - Multicast traffic may be punted to the RP with the "no group" reason, even if (*,G) and (S,G) exist on the PXF. You can observe the punted traffic in the output of the **show hardware pxf cpu statistics diversion** command.

  - PIM neighbors across an MDT in an MVPN network may flap.

  Conditions: This symptom is rarely observed when either PXF or the router is rebooted or reloaded while traffic runs in the network. When the router has a large configuration or when many multicast streams pass through the router, the probability of the symptom occurring increases.

  Workaround: Make a note of the traffic streams that are punted to the RP by entering the **show hardware pxf cpu statistics spd** command. Then, clear these traffic streams by entering the **clear ip mroute** *group* command.

  When the multicast routing table is small, just enter the **clear ip mroute *** command.

  Further Problem Description: The packets that are punted to the RP are rate-limited by a multicast data traffic SPD process. These packets are counted as "no group".

  In an MVPN network, control plane traffic is encapsulated in an MDT. If this MDT traffic is punted and rate-limited, the control plane traffic is lost, causing PIM neighbors to flap.

- CSCeh23047

  Symptoms: After a manual SSO switchover, traffic in the tag switching-to-IP switching direction between an egress 1-port 10-Gigabit Ethernet Engine 4+ line card and an ingress 4-port Gigabit Ethernet ISE line card does not recover.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(31)S.

  Workaround: Reload microcode onto the 4-port Gigabit Ethernet ISE line card.

- CSCeh27734

  Symptoms: For recursive routes with implicit null as the local label, the FIB may point to the rewrite of the parent prefix. However, this situation may not affect any functionality.

  Conditions: This symptom is observed on a router that is configured for MPLS forwarding.

  Workaround: Change the affected prefix to be non-recursive.

- CSCeh29983

  Symptoms: Several crashes have occurred in multiple VIP's on a Cisco 7513.

  Conditions: No conditions which lead to this event have been discovered so far.

  Workaround: There is no workaround.

- CSCeh33574

  Symptoms: An Engine 4 plus or Engine 5 line card does not come up.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(31)S when IPC timeout errors occur.

  Workaround: There is no workaround.

- CSCeh34989

  Symptoms: One of the following two symptoms may occur on a POS ISE egress line card:

  - The interface may become stuck during transmission. The line protocol will continuously flap because the interface continues to receive keepalives but is not able to send any keepalives.

  - The line card generates the following harmless error message:

  ```
  %EE48-4-GULF_TX_SRAM_ERROR: ASIC GULF: TX bad packet header detected. Details=0x4000
  ```

  Conditions: These symptoms are observed on a Cisco 12000 series when an invalid packet is forwarded to an egress interface on an ISE line card.

  Workaround: If the transmission on the interface is stuck, reload the line card by entering the **hw-module slot** *x* **reload** command.

- CSCeh36824

  Symptoms: When the HA mode is RPR+ and a standby PRE comes up after a crash, the HA mode may change from RPR+ to SSO and the standby PRE displays error messages that indicate that the running configuration of the active PRE is "mode rpr-plus" but the running configuration of the standby PRE is "mode sso."

  When the HA mode is SSO and a standby PRE comes up after a crash, the standby PRE may become stuck in its initialization and does not enter the "STANDBY_HOT" state.

  Conditions: These symptoms are observed on a Cisco 10000 series when the standby PRE crashes but does not report a switchover (that is, a "standby down" event occurs but not a switchover event), causing the standby PRE to come up in an inconsistent state. When the standby PRE crashes, the active PRE shows an error message that includes the text "PEER_CRASH_INTERRUPT."

Workaround: Reset the standby PRE by entering the **hw-module standby-cpu reset** command to enable it to reload and come back up properly.

- CSCeh37351

  Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

  - tag2ip, with bad ip hdr cksum
  - tag2ip, with ip->tl > L2
  - tag2ip, with ip->tl < 20
  - tag2ip, with ip options packets
  - tag2ip, with ip options packets with bad ip hdr cksum
  - tag2ip, with ip options packets with ip->tl > L2
  - tag2ip, with ip options packets with ip->tl < 20

  These bad packets cause packet corruption and an "TX192-3-PAM_PIM" error message on the E4+ line card and may even cause the E4+ line card to reset.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh42465

  Symptoms: An Engine 3 line card sends unlabeled traffic after it has been toggled from explicit routing to default routing. The symptom is related to the handling of a default-route on an Engine 3 ingress line card that functions in an IP-to-MPLS path.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(30)S1 or any other image that includes the fix for caveat CSCsa64782, which is a preliminary requisite for default-route handling on an Engine 3 line card. The symptom occurs in the following scenario:

  1) You configure BGP to advertise the target address, so the target address is directly known in the routing table.

  2) You remove the advertisement from BGP and return to default routing, with the same source for the next hop as the platform that was the BGP next hop.

  3) You enter the **clear ip route** *network* command, with the address of the BGP next hop for the *network* argument.

  After the transition from non-default routing to default routing, entering the **clear ip route** *network* command, with the address of the next hop for the *network* argument, causes an inconsistency, and traffic is forwarded as unlabeled.

  Workaround: To restore proper operation, enter the **clear ip route 0.0.0.0** command.

- CSCeh46072

  Symptoms: When the following sequence if performed on a GSR, multiple subinterfaces will end up with the same ifnumber, thus resulting in incorrect CEF entries:

  1. add serial subinterface (channelized). 2. delete the interface created. 3. add ATM subinterface. 4. add back the serial subinterface.

Conditions: This symptom occurs only if the above (or similar) sequence of adding and deleting subinterface is done.

Workaround: Do not delete and re-add the same subinterface. Instead, enter the **shut** command and then the **no shut** command. The same effect is achieved without running into the above symptom.

- CSCeh49881

  Symptoms: In a tag switching-to-IP switching scenario with an ISE ingress line card and an Engine 4 plus (E4+) egress line card, the following bad packets may be forwarded to the E4+ line card:

  - tag2ip, with bad ip hdr cksum
  - tag2ip, with ip->tl > L2
  - tag2ip, with ip->tl < 20
  - tag2ip, with ip options packets
  - tag2ip, with ip options packets with bad ip hdr cksum
  - tag2ip, with ip options packets with ip->tl > L2
  - tag2ip, with ip options packets with ip->tl < 20

  These bad packets cause packet corruption and an "TX192-3-PAM_PIM" error message on the E4+ line card and may even cause the E4+ line card to reset.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the ISE line card to drop the above-mentioned bad packets.

- CSCeh60185

  Symptoms: An Engine 4 plus (E4+) line card that functions in an IP-to-tag switching scenario may generate "TX192-3-PAM_MODULE" and "%TX192-3-PAM_PIM" error messages and tracebacks or may crash.

  Conditions: This symptom is observed on a Cisco 12000 series when the ingress interface is an Engine 2 line card that has an input ACL and when an external LDP flap occurs that affects the Engine 4+ line card.

  Workaround: There is no workaround.

- CSCin67741

  Symptoms: The Route Processor (RP) crashes when encapsulation is removed using the **no encapsulation** command.

  Condtions: This symptom has been observed on a multilink interface with DLFI configuration under traffic.

  Workaround: There is no workaround.

- CSCin87776

  Symptoms: Multilink bundles on a Cisco 7500 series may process-switch traffic instead of using dCEF, causing the CPU usage of the RSP to increase sharply and a CPU hog condition to occur.

  Conditions: This symptom is observed when an RPR+ switchover occurs on a Cisco 7500 series that is configured for HA.(The switchover causes an MLP to flap.) However, the symptom may also occur on a Cisco 7500 series that has a single RP (so, without a switchover) when an MLP link flaps.

Workaround: There is no workaround. Note that the symptom does not occur when SSO is configured because the MLP state is maintained.

- CSCin88273

  Symptoms: After an RPR+ or SSO switchover occurs, an MLP sequence number mismatch may occur, a ping between back-to-back interfaces may not go through, and the routing protocol through this link may go down.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for dMLP and RPR+ or SSO.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the multilink interface of the Cisco 7500 series.

- CSCin88303

  Symptoms: The line protocol of unchannelized interfaces on a PA-MC-2T3+ port adaptor remains down although the link is up.

  Conditions: This is observed when you change from the channelized mode to the unchannelized mode by entering the **no channelized** command on the T3 controller of the PA-MC-2T3+ port adaptor.

  Workaround: There is no workaround.

- CSCin88356

  Symptoms: The output of the **show interfaces serial** *number* command does not show the total output packet drops.

  Conditions: This symptom is observed when you apply a service policy on an interface that is configured for CEF.

  Workaround: Enter the **show policy map interface** *interface-name* command to see the total output packet drops.

- CSCsa41907

  Symptoms: When a channel group is removed from and added to a controller and when a PRE switchover occurs, the line protocol on another channel goes down after a while and input packets are not counted.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 6-port channelized T3 line card.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

  Alternate Workaround: Ensure that the you enter the **hw-module standby-cpu reset** command before a PRE switchover occurs.

- CSCsa46887

  Symptoms: A router builds an Echo Reply that is invalid and may be misunderstood.

  Conditions: This symptom is observed on a router that is configured for LSPV when the router receives an Echo Request with a Pad TLV that has a value of "Copy Pad TLV to reply." The Echo Reply that the router builds includes residual data from previously received packets instead of the pad pattern that was received.

  Workaround: There is no workaround.

- CSCsa49740

  Symptoms: Packets are punted to the GRP at a rate of 5000 pps, causing the CPU utilization of the CPU to reach more than 50 percent.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 when a 4-port Packet-over-SONET OC-48c Engine 4 plus line card (4OC48E/POS-SR-SC=) receives TCP packets with destination 0.0.0.0.

  Workaround: There is no workaround.

- CSCsa49906

  Symptoms: When loopback is removed from a T1 interface of a CT3 controller, the following warning message is encountered with a removal of the loopback being denied:

```
GSR(config)#cont t3 7/5
GSR(config-controller)#no T1 5 loopback
%Inband loopback is already running on T1 12. Only one code can be running per
T3 at a time
GSR(config-controller)#
```

  Conditions: The symptom is observed after upgrading to Cisco IOS Release 12.0 (27)S2 on a Cisco 12000 Series Gigabit Switch Router with a 6CT3 linecard.

  Workaround: There is no workaround.

- CSCsa54891

  Symptoms: Under normal operation, an Engine 6 line card may reset with the following error messages and tracebacks:

```
%TX192-3-CPUIF: Error=0x10
rd 0x73 base 0x73 hdr 0x75 last 0x75 wr 0x75 insert 0x0 back 0x0 len 0x2474 cnt 0x0
-Traceback= 40D89758 405A9008 405EC67C 406D5E7C 406D64F8 400FC020
%TX192-3-CPUIF_ERR: FIFO RAM3 Parity Error.
-Traceback= 40D89808 405A9008 405EC67C 406D5E7C 406D64F8 400FC020
%GSR-3-INTPROC: Process Traceback= 400FFD20 400FCAA0 40010F6C
-Traceback= 404EFBCC 406D6760 400FC020
%FABRIC-3-ERR_HANDLE: Due to FIA HALT error, reconfigure FIA on slot 9
```

  Conditions: This symptom is observed on a Cisco 12000 series when false RAM parity errors occur.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat determines whether the RAM parity errors are real or false.

- CSCsa56142

  Symptoms: Entering the **no export map** VRF configuration mode command has no effect.

  Conditions: This symptom is observed on a Cisco router that is configured for RPR+ or SSO when the you take the following steps:

  1) You enter the **no export map** VRF configuration mode command on the active RP.

  2) You enter the **write memory** command.

  3) You initiate an RPR+ or SSO switchover.

  After these steps, the export map is still configured on the new active RP, while it should no longer be present.

Workaround: Manually remove the export map from the new active RP.

- CSCsa58340

  Symptoms: Upon entering the **police** command, the router reloads unexpectedly.

  Conditions: The reload occurs if the policy map being edited already contains the maximum number of classes that the Cisco 10000 supports and the user attempts to add one more class with police.

  Workaround: Avoid using policy maps that contain more classes than what the Cisco 10000 supports.

- CSCsa59002

  Symptoms: IP fragments with a User Datagram Protocol (UDP) protocol identifier may be improperly denied on an Engine 3 line card that has an outbound access control list (ACL) that denies specific UDP ports.

  Conditions: This symptom is observed only for outbound ACLs on an Engine 3 line card on a Cisco 12000 series. The following is an example of an ACL statement for which the symptom may occur:

  ```
  access-list 100 deny udp any any eq 0 <<< this line may accidently deny IP
  fragments for UDP access-list 100 permit ip any any
  ```

  Workaround: Use the following ACL instead of the above-mentioned example:

  ```
  access-list 101 permit udp any any fragments
  access-list 101 deny udp any any eq 0
  access-list 101 permit ip any any
  ```

- CSCsa59109

  Symptoms: At random, subinterfaces loose the ability to ping a directly-connected peer.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured with two 3-port Gigabit Ethernet line cards.

  Note that although regular and extended pings do not work, pings that use the record option do work.

  Workaround: Reload microcode onto the affected line cards.

- CSCsa59829

  Symptoms: With traffic passing over a network only occasionally, a 4-port OC12 ATM ISE line card generates a "%PM622-3-CPK24_INTR: Egr SAR timeout" error message and resets.

  Conditions: This symptom is observed on a Cisco 12000 series.

  Workaround: Reload the line card.

  Further Problem Description: The symptom occurs when the "CPK24 FPGA" detects that the SAR does not respond in the "Utopia interface." The SAR then crashes because of a bad canonical header in the egress direction.

- CSCsa64782

  Symptoms: When an ingress ISE line card is used with a default route that iBGP learns over a MPLS core, the following two symptoms may occur:

  - The output of the **show controllers tofab alpha mip stat | i MTU** command may show traffic drops.

  - Traffic is incorrectly sent as "unlabeled" over the MPLS core.

  Conditions: These symptoms are observed on a Cisco 12000 series when the traffic path follows a recursive default route and when recursive load sharing occurs.

  Workaround: Prevent outbound load sharing to the default route by changing the IGP metrics.

- CSCsa65732

  Symptoms: When you remove a policy map from a subinterface, the subinterface may become stuck, preventing traffic from passing through the subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX7 when a nested policy map is applied to the main or physical interface in addition to the one that is already applied to the subinterface. The symptom could also occur in Release 12.0S.

  Workaround: Remove the policy map from the physical interface before you remove the policy map from the subinterface. When the subinterface configuration is updated, re-apply the policy map to the physical interface.

- CSCsa67488

  Symptoms: A Cisco 10008 router with PRE1 may report a PXF crash.

  Conditions: The symptom is observed when modifying an access-list that is already attached to a multilink interface.

  Workaround: Modify an access-list only if it not attached to the interface. If the access-list cannot be removed from the interface, then create a new one and apply.

- CSCsa68301

  Symptoms: Inter-MVPN traffic does not function on an Engine 4+ line card.

  Conditions: This symptom is observed on a Cisco 12000 series and may occur with any Engine 4+ line card.

  Workaround: There is no workaround.

- CSCsa68616

  Symptoms: An IPC failure occurs and an OC-12 line card that is configured for Frame Relay over MPLS resets.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

  Workaround: There is no workaround.

  Further Problem Description: The IPC failure and the line card reset occur after a depletion of the elements in the FrFab 608 byte queue for the line card. Consecutive outputs of the **show controllers** *slot-number* **frfab queue** command show a consistent and rapid leak of these buffers.

- CSCsa70274

  Symptoms: A Cisco router may crash during an LSP traceroute when a transit router responds with a downstream map TLV that contains a multipath length field that is set to 0, 1, 2, or 3.

  Conditions: This symptom is observed during testing of the Cisco LSP ping draft version 3 in a network that uses a later version of the LSP ping draft.

  The implementation of draft version 3 does not handle the multipath length field settings correctly. In draft version 3 and earlier drafts, there is an ambiguity on whether or not the multipath length field includes the four bytes comprising of the hash-key type, depth limit, and multipath length fields. As such, all implementations of the draft version 3 encode the length as four bytes and reply with a multipath length of four bytes.

When an LSP traceroute is invoked and a transit router replies with a downstream map TLV that contains a multipath length field that is set to a length shorter than four bytes, existing implementations handle this situation incorrectly and cause memory packet memory to become corrupted during the subsequent attempt to build an MPLS echo request packet. This situation eventually causes the router to crash.

Workaround: If LSP traceroute implementations exist on a transit router that cause the transit router to reply with a multipath length that is set to a value other than four, avoid using an LSP traceroute.

Note, however, that the implementations of Cisco LSP ping draft version 3 do not reply with multipath lengths that can cause this crash.

Wide-Area Networking

- CSCeh33185

  Symptoms: A POS interface on a VIP4-80 that is configured for PPP goes down and remains down.

  Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0S only when PPP receives an LCP PROTOCOL REJECT message for PAP or CHAP. The symptom may also occur in other releases.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the afected POS interface.

- CSCsa49019

  Symptoms: A memory leak may occur in the "Multilink Events" process, which can be seen in the output of the **show memory summary** command:

```
0x60BC47D0 0000000024 0000000157 0000003768    MLP bundle name
0x60BC47D0 0000000028 0000000003 0000000084    MLP bundle name
0x60BC47D0 0000000044 0000000001 0000000044    MLP bundle name
0x60BC47D0 0000000048 0000000001 0000000048    MLP bundle name
0x60BC47D0 0000000060 0000000001 0000000060    MLP bundle name
0x60BC47D0 0000000064 0000000013 0000000832    MLP bundle name
0x60BC47D0 0000000068 0000000008 0000000544    MLP bundle name
0x60BC47D0 0000000072 0000000001 0000000072    MLP bundle name
0x60BC47D0 0000000076 0000000001 0000000076    MLP bundle name
0x60BC47D0 0000000088 0000000018 0000001584    MLP bundle name
```

  Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(27)S4

Cisco IOS Release 12.0(27)S4 is a rebuild of Cisco IOS Release 12.0(27)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(27)S4 but may be open in previous Cisco IOS releases. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdz61503

  Symptoms: A Cisco router may reload when it performs Simple Network Management Protocol (SNMP) Notification Log MIB queries.

  Conditions: This symptom is observed on all versions of Cisco IOS software. The symptoms are not observed on a Cisco ONS 15530 or a Cisco ONS 15540 switch module because the symptoms have been resolved on these platforms.

  Workaround: Exclude the NOTIFICATION-LOG-MIB.

- CSCec87661

  Symptoms: A “SYS-2-CHUNKBOUNDS” error message may be displayed on the router console. This message may be followed by a “NOTQ” error message.

  Conditions: This symptom is observed under rare circumstances during heavy usage of any application that is using chunks. The symptom is platform independent.

  Workaround: There is no workaround.

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial-In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml.

- CSCee87891

  Symptoms: SNMP entries may be deleted when you configure SNMP or when you reload the router on which SNMP is configured.

  Conditions: This symptom is observed when an SNMP user is configured with the same name or host name as a community.

  Workaround: There is no workaround.

- CSCee95282

  Symptoms: A router may generate a very large remote processing time report that may take between 10 and 25 seconds to be generated.

Conditions: This symptom is observed when you enter the **rtr responder** command for the first time and you do not reload the router.

Workaround: Reload the router after you have entered the **rtr responder** command.

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

Interfaces and Bridging

- CSCed65436

  Symptoms: A Cisco router may report spurious accesses when configured for Multilink PPP (MLPPP). This appears to be caused by fragmentation.

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at [hex] reading [hex] %ALIGN-3-TRACE:
  -Traceback=[hex]
  ```

  Conditions: MLPPP must be configured for this symptom to occur.

  Workaround: There is no workaround.

- CSCee25605

  Symptoms: When you enter the **show ip interface brief**, the output indicates that a serial subinterface has a down status and that the protocol is down too:

  ```
  router# show ip interface brief
  Interface     IP-Address      OK? Method Status                Protocol
  Ethernet0/0   10.7.0.68       YES NVRAM  up                    up
  Ethernet0/1   unassigned      YES NVRAM  administratively down down
  Ethernet0/2   unassigned      YES NVRAM  administratively down down
  Ethernet0/3   unassigned      YES NVRAM  administratively down down
  Ethernet0/4   unassigned      YES NVRAM  administratively down down
  Ethernet0/5   unassigned      YES NVRAM  administratively down down
  Serial4/0     unassigned      YES NVRAM  administratively down down
  Serial4/1     unassigned      YES NVRAM  administratively down down
  Serial4/2     unassigned      YES NVRAM  administratively down down
  Serial4/3     unassigned      YES NVRAM  administratively down down
  Serial4/4     unassigned      YES NVRAM  administratively down down
  Serial4/5     unassigned      YES NVRAM  administratively down down
  Serial4/6     unassigned      YES NVRAM  administratively down down
  Serial4/7     unassigned      YES NVRAM  administratively down down
  Serial5/0:23  10.0.0.1        YES NVRAM  down                  down
  ```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 when you attempt to configure the interface and bring it up.

Workaround: There is no workaround.

- CSCef79968

  Symptoms: When an snmpget is executed for an interface index below .1.3.6.1.2.1.31.1.1.1.6, the router responds with the following information:

  ```
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.12 : VARBIND EXCEPTION: No Such Instance
  ```

  However, an snmpwalk executes successfully for an interface index below .1.3.6.1.2.1.31.1.1.1.6.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 when an snmpget is executed for 4GE-SFP-LC subinterfaces or for an 4GE-SFP-LC interface when there is another interface index for the same interface. The symptom may be platform-independent.

  Workaround: Reload the router.

IP Routing Protocols

- CSCed46066

  Symptoms: When both VRF and non-VRF processes are configured and both processes have the **redistribute** command enabled, removal of the **redistribute** command from one process may also disable redistribution for the other process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(27)S or Release 12.3(4)T.

  Workaround: Reconfigure the **redistribute** command for the process for which the command should not have been disabled.

- CSCed59978

  Symptoms: A router may crash and reload due to a bus error, and the following error message may appear:

  ```
  Unexpected exception, CPU signal 10
  ```

  Conditions: This symptom is observed on a Cisco router that is running OSPF and that is configured for incremental SPF.

  Workaround: Remove incremental SPF from the router by entering the **router ospf** *process-id* command followed by the **no ispf** command.

- CSCee28148

  Symptoms: After a switchover on a router, one or more obsolete LSAs from a neighboring router may still be present in the topology. This is improper behavior: the LSAs should no longer be present in the topology.

  Conditions: This symptom is observed when a switchover occur on a Cisco router that runs OSPF NSF and when a neighboring router flushes one or more of its self-originated LSAs.

  Note that the LSAs automatically age out within an hour, unless the link that connects the router and the neighboring router is a demand circuit or has OSPF “flood-reduction” configured.

  Workaround: If the LSA is an external LSA (type5/type7), enter the **clear ip ospf redistribution** command on the neighboring router. In all other cases, enter the **clear ip ospf process** command on the neighboring router.

- CSCee35125

  Symptoms: A Cisco router may crash when you enter the **clear ip route *** command.

  Conditions: This symptom is observed when the routing table has a default route.

  Workaround: There is no workaround.

- CSCee67450

  A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the **bgp log-neighbor-changes** command configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  If a misformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the **show ip bgp neighbors** command or running the **debug ip bgp** *neighbor* **updates** command for a configured BGP neighbor.

  Cisco has made free software available to address this problem.

  For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml

- CSCee85676

  Symptoms: When VPNv4 route advertisement are received after BGP has converged, the existing path is updated but imported paths from the original path are not updated accordingly.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the **maximum-paths** *number-of-paths* **import** *number-of-paths* command is enabled. The symptom occurs when the path attributes are changed dynamically instead of the path being completely withdrawn and readvertised.

  Workaround: Withdraw the prefix from the remote PE router and then readvertise the prefix.

- CSCee86530

  Symptoms: A BGP update that is sent to a connected P router fails to report the martian next-hop log message when the next-hop field in the attribute of the BGP update is set to 255.255.255.255 (that is, all 1ís). The P router does deny the advertisement of the MP_REACH_NLRI attribute to the other PE routers, but there is no log message to indicate that it is denying the advertisement and why it does so.

  Conditions: This symptom is observed during MP-BGP negative testing for the MP_REACH attribute.

  Workaround: There is no workaround.

- CSCef91275

  Symptoms: An MPLS TE tunnel stays stuck in the “Path Half Admitting” state, as is shown by the output of the **show mpls traffic-eng tunnel** command, thereby preventing the tunnel from coming up.

  Conditions: This symptom may be observed when a particular third-party router that functions as the headend for the MPLS TE tunnel sends a Path message to a Cisco router that functions as the midpoint for the router MPLS TE tunnel and that does not have the **mpls traffic-eng tunnels** interface configuration command enabled on the outbound interface that would be used to forward the Path message.

Workaround: Enter the **mpls traffic-eng tunnels** interface configuration command on the outbound interface of the Cisco router. Then, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on this interface, and save the configuration.

- CSCef92863

  Symptoms: A Cisco 10000 PRE-1 may reload when a VRF that is configured with eight maximum paths is modified.

  Conditions: This symptom is observed when a VRF on the Cisco 10000 series is configured for eight maximum EIBGP paths by entering the **maximum-paths eibgp 8** command and when the VRF is modified in such a way that there is a change in the number of paths that are available. The symptom may also occur on a Cisco 10720.

  Workaround: A Cisco 10000 series can support only six maximum paths. Therefore, configure the number of maximum paths by entering the **maximum-paths eibgp 6** command.

ISO CLNS

- CSCeg00610

  Symptoms: A router running Cisco IOS software may reload unexpectedly.

  Conditions: This symptom has occurred when running those versions of software with the Integrated Intermediate System-to-Intermediate System (IS-IS) Incremental shortest path first (SPF) feature and when IS-IS Incremental SPF feature is enabled to run.

  Workaround: Disabled IS-IS Incremental SPF.

Miscellaneous

- CSCed16318

  Symptoms: When changing the MTU on an Engine 2 3-port 1GE line card, the line card may reload.

  Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(26)S.

  Workaround: Ensure there is no traffic going through the Engine 2 3-port 1GE line card when attempting to change the MTU.

- CSCed57204

  Symptoms: When a large number of VRFs are configured, input OAM F5 loopback cells on the ATM interface are dropped continuously even without traffic. Drop could be seen at OAM cell drops of **show atm traffic** and at Input queue drops of **show interface ATM** EXEC commands.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(19), Release 12.3(5), or Release 12.3(4)T2 where the **oam-pvc manage** command and the **ip vrf** global command are configured.

  Workaround: Remove the **ip vrf** command. There is no workaround for a router such as a provider edge (PE) router that cannot remove VRFs.

- CSCed81317

  Symptoms: With the import map configured on the VPN Routing and Forwarding (VRF), even the CE-learned routes (non-eBGP) are getting filtered out so they will never appear in the VRF routing table.

  Conditions: Under VRF configuration, **import map** *word* needs to be configured. Due to the symptom, this filter is applied to CE-learned routes with the exception of eBGP routes.

Workaround: There is no workaround.

- CSCed82964

  Symptoms: L2 loadbalancing might be affected on an egress link bundle.

  Conditions: This symptom is observed a Cisco 12000 series when the ingress interface is a regular Engine 2 interface and when the member interfaces in the bundle are toggled.

  Workaround: Enter the config mode of the port channel and exit.

- CSCee16205

  Symptoms: The committed information rate (CIR), normal burst, and maximum burst of the **police** (percent) command in a policy map are set incorrectly.

  Conditions: This symptom is observed when the policy map is attached to an MLP interface that is configured for LFI and that is in the "DOWN" state.

  Workaround: Attach the policy map when the MLP interface is in the "UP" state.

- CSCee16725

  Symptoms: MPLS VPN VRF labels fail to be updated onto core-facing line cards such that the VPN traffic entering the core-facing line cards is punted to the RP.

  Conditions: This symptom is observed in a setup with two parallel paths between a PE router and a CE router that run Cisco IOS Release 12.0 S. There are around 10,000 VRF routes advertised through both the eBGP sessions that are established between the PE router and the CE router. When the link flaps, the next hop of all the BGP routes changes to the next hop via the other link. When this situation occurs, the core-facing line cards may miss the label forwarding entry for some of the VPN prefixes.

  Workaround: To recover from the problem after it has occurred, enter the **clear cef linecard** command on the affected core-facing line card.

  To avoid the problem from occurring, do not redistribute the PE-CE link subnet into BGP.

- CSCee19222

  Symptoms: An MLP bundle configured between a Cisco 7500 series and any other router may not be able to switch traffic when dCEF is enabled on the Cisco 7500 series.

  Conditions: This symptom is observed when LFI is enabled with one member link in the MLP bundle.

  Workaround: Either remove dCEF or remove LFI. (A combination of CEF and MLP is not supported.) Note that if there are two member links in the interleaving-enabled MLP bundle, the problem does not occur.

- CSCee27276

  Symptoms: A router shows a constant increase in the holding memory for the L2TP Daemon process.

  Conditions: This symptom is observed when invalid L2PTv3 control packets are sent from a peer router. Invalid packets means packets without all the mandatory attribute value pairs.

  Workaround: There is no workaround.

- CSCee31196

  Symptoms: An LDP session over a tunnel interface may drop and not come back up.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.0(27)S1 when auto-tunnel traffic engineering is configured and when RSVP label distribution is configured in the MPLS core.

Workaround: Run LDP in the MPLS core for all interfaces that have auto-tunnel traffic engineering configured.

- CSCee32365

  Symptoms: When a single bundle link associated with a Multilink Frame Relay (MFR) interface is brought up, LMI exchanges over the MFR interfaces may not happen.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for MFR.

  Workaround: There is no workaround.

- CSCee34622

  Symptoms: Neighbor adjacencies for the IS-IS, OSPF, or other routing protocol may bounce during a Nonstop Forwarding (NSF) switchover.

  Conditions: This symptom is observed when you enable a routing protocol for NSF and you enter the **external overload signalling** router configuration command. The following configuration illustrates this situation for IS-IS:

  router isis *area-tag* **nsf [cisco | ietf] external overload signalling**

  Workaround: Disable the **external overload signalling** router configuration command.

- CSCee47026

  Symptoms: The ATM HA process may crash.

  Conditions: This symptom is observed on a Cisco router that has VCS configured with local switching.

  Workaround: There is no workaround.

- CSCee49862

  Symptoms: A Cisco 7500 series multichannel T3 port adapter (PA-MC-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCee51909

  Symptoms: An Engine 3 channelized (OC-48 to DS3) line card that processes traffic crashes.

  Conditions: This symptom is observed when you change the MTU on the E4+ disposition line card.

  Workaround: There is no workaround.

- CSCee53458

  Symptoms: After you boot a Cisco 12000 series, one of the members of a link bundle that has eight members that are configured on an Engine 2 16-port O-C3 POS line card shows up in both the active and passive lists.

  Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release of Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

  Further Problem Description: Proper functionality is not impacted by this caveat.

- CSCee69887

  Symptoms: A dual SRP ring fails to become active completely due to an is-type mismatch. The output of the **show clns neighbors** command indicates that a certain system interface remains in the "Init" state indefinitely, although the output of the **show ip interface brief** command shows that this interface is up.

  Conditions: This symptom is observed when a dual SRP ring is configured on three routers that run Cisco IOS Release 12.2S. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCee70591

  Symptoms: A Cisco 7500 series T3 port adapter (PA-2T3+) may not provide a two-second delay before bringing down the T3 controller.

  Conditions: This symptom is observed when an alarm as defined in the ANSI T1.231 specification occurs.

  Workaround: There is no workaround.

- CSCee72906

  Symptoms: A VIP may crash when you remove a service policy from a multilink interface or when a member link is removed from the multilink interface while heavy traffic is being processed.

  Conditions: This symptom is observed on a Cisco 7500 series that has an RSP and that is configured for dLFI over a leased line, MLP, and QoS.

  Workaround: There is no workaround.

- CSCee73410

  Symptoms: When you enter the **redundancy force-switchover** command, IPC messages and tracebacks may be generated on an Engine 2 3-port GE line card.

  Conditions: The symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S or an earlier release and that has dual GRPs or dual PRPs.

  Workaround: There is no workaround.

- CSCee79728

  Symptoms: A Cisco 7200 series that operates in the process switching path may crash with a bus error exception.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(13b)M2 and that is configured with a serial or POS port adapter. The symptom may also occur in other releases.

  Workaround: Enter the **ip route cache** command for all interfaces.

- CSCee83781

  Symptoms: A Cisco router may reload when you enter the **show ipv6 mfib verbose** command for a large MFIB.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for multicast.

  Workaround: There is no workaround.

- CSCee84732

  Symptoms: The CPU utilization of a router that is configured for Multiprotocol Label Switching (MPLS) may temporarily increase to 80 or 90 percent when a peer router is reloaded or when an interface with a large number of numbered subinterfaces is administratively enabled.

Conditions: The symptom is observed in a rare situation when label distribution protocol (LDP) is used in configurations with a very large number of numbered interfaces. When this problem occurs, the output of the **show process cpu sorted** command shows that the "Tagcon Addr" process consumes the majority of the CPU cycles.

Workaround: There is no workaround.

- CSCef06050

  Symptoms: IPv6 unicast and multicast traffic may not recover on an Engine 4 plus (E4+) 1x10 GE line card after you have performed two software OIRs of the primary CSC.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0S.

  Workaround: Reload the E4+ 1x10 GE line card.

- CSCef06121

  Symptoms: An Engine 2 3-port Gigabit Ethernet line card may stop transmitting packets.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(24)S6.

  Workaround: Enter the **hw-module reload** command to enable the line card to resume transmitting packets.

- CSCef06858

  Symptoms: Line cards in a Cisco 12000 series may fail when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured with two PRPs and that runs a Cisco IOS interim release for Release 12.0(30)S when you enter the **redundancy force-switchover** command. Note, however, that this caveat is resolved in Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCef18515

  Symptoms: After you have entered the **clear cef line** command, when you enter the **show ip cef** command for the RP and for a line card, the output is inconsistent.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that is configured for Fast ReRoute.

  Workaround: There is no workaround.

- CSCef22069

  Symptoms: On a Cisco 12000 series that functions as an egress PE router in an MPLS VPN network, after the customer-facing Gigabit Ethernet line card is reloaded, the ingress line card that receives an incoming VPN label with a destination with a glean adjacency (which requires an ARP) without a BGP session may not properly complete the adjacency, causing traffic to be dropped.

  Conditions: This symptom is mostly observed with static recursive route configurations. To recover from the symptom, manually ping the interface of the CE router from the adjacent PE router.

  Workaround: Configure the static ARP entries for the nexthop router that is configured in the static recursive routes.

- CSCef25917

  Symptoms: A 4GE-SFP-LC line card may reload unexpectedly when it processes QoS traffic in a configuration with a VLAN on a VCG that is configured with an ingress CoS.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or a later release when the resolved ARPs are deleted, for example, when routers flap, when BGP peers do not respond, or when you enter the **clear arp** command. Note that the symptom may also occur on releases earlier than Release 12.0(26)S.

The ingress CoS includes a **set** command for the matched class: either a **police** command with a **set** command or a simple **set** command and either a **set-mpls** command or a **set-dscp** command.

Possible Workaround: Configure static ARPs.

- CSCef26543

  Symptoms: A Cisco 12000 series line card may rate-limit process-switched packets to the GRP. This situation causes a ping to be lost when you perform a ping test to the local interface of the router.

  Conditions: This symptom is observed when the interface is configured for HDLC, when the interface has a hard loop, and when the IP address of the interface is the destination of the ping. Because the interface is in the up/up state (looped) and functional, there should be no packet loss when you ping the interface at its own IP address.

  Workaround: There is no workaround.

- CSCef29467

  Symptoms: When you enter commands in various configuration modes such as address-family, PVC, service-policy, and so on, an invalid input error message may be returned even though the command was accepted and entered into the running configuration. The following is an example:

  ```
  Router(config-router-af)#redistribute connected
  address-family ipv4 vrf atmTrk
   ^
  % Invalid input detected at '^' marker.
  ```

  Conditions: This symptom is observed on a Cisco 12410 that is configured with two Performance Route Processors (PRP-1) that function in Route Processor Redundancy (RPR) mode and that runs one of the following images:

  - The c12kprp-p-mz image of Cisco IOS Release 12.0(24)S3.

  - The c12kprp-p-mz image of Cisco IOS Release 12.0(23)S4.

  - The c12kprp-k3p-mz image of Cisco IOS Release 12.0(27)S2

  This list is not all-inclusive: the symptom may also occur in Release 12.0(20)S, Release 12.0(20)ST, and later releases.

  The symptom occurs when the **do** command is interleaved between configuration commands.

  Workaround: Verify that the configuration command is properly accepted by entering the **show running-config** command.

- CSCef33670

  Symptoms: An Engine 4 egress line card that switches traffic may reset when the ingress line card is shut down.

  Conditions: This symptom is observed on a Cisco 12000 series when the ingress line card is an Engine 3 POS line card and when IP-to-tag traffic is switched.

  Workaround: There is no workaround.

- CSCef39284

  Symptoms: A router may crash when you enter the **crypto key generate dss** *key-name* command.

Conditions: This symptom is observed on a Cisco 12012 that is configured for SSH but may occur on any Cisco platform that is configured for SSH.

Workaround: There is no workaround.

- CSCef53169

  Symptoms: An outbound ACL with a log/log-input keyword changes the IP destination address in the packets. As the result, packets that should be permitted are incorrectly denied.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(29)S when the incoming interface for the packets is a tag-switching interface. The symptom is observed irrespective of whether the interface with this outbound ACL is a tag-switching interface or not.

  Workaround: Do not use the log/log-input keyword in the ACL.

- CSCef53570

  Symptoms: When IPv4 multicast is configured on an interface and when hardware forwarding is enabled, the interface stops forwarding all unicast and multicast traffic.

  Conditions: This symptom is observed only on Cisco 12000 series Engine 2 line cards.

  Workaround: Disable hardware forwarding.

- CSCef54779

  Symptoms: Under a rare condition, when a main interface switches over to a backup interface on 4-port GE line card, a ping to another neighboring interface that is not at all related to the backup interface fails. A sniffer trace shows that the Src/Dst MAC address in the ICMP reply is that of the backup interface.

  Conditions: This symptom is observed on a Cisco 12000 series when you repeatedly disable the main interface that is associated with a backup interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCef67078

  Symptoms: A PXF buffer leak occurs on an L2TPv3 decapsulation router, which van be observed in the output of the **show hardware pxf cpu buffer** command:

```
router#show hardware pxf cpu buffer
FP buffers
pool   size    # buffer    available   allocate failures    low buffer drops
------------------------------------------------------------------------------
0      9344    1293        1293        0                    0
1      1664    12930       12930       0                    0
2      640     26746       127         0                    77165
3      256     34072       34072       0                    0
4      128     59934       59934       0                    0
```

  Depending on the packet size, the buffer leak can occur in different pools.

  Conditions: The symptom is observed on a Cisco 10720 in the following two scenarios:

  - An MPLS-enabled interface is the network backbone for L2TPv3 tunnels.

  - An 802.1q interface is the network backbone for L2TPv3 tunnels and an input security ACL with more than 400 lines is configured on the 802.1q backbone interface.

  Workaround: There is no workaround.

- CSCef67267

  Symptoms: The Fast ReRoute database shows all prefixes in the active state.

  Conditions: This symptom is observed on a Cisco router after a connected point of local repair (PLR) has rebooted.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the primary tunnel is configured. Doing so restores the prefixes to the ready state.

- CSCef67840

  Symptoms: When the CEF table consistency checker is configured to perform a passive scan check of tables of the line cards, the CEF table consistency checker may report false inconsistencies, which you can view in the output of the **show ip cef** *ip-address* command. The false inconsistencies may occur because of a race condition.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1.

  If an inconsistency is reported for a recursive loadbalanced route for which the output interfaces for the next-hop IP address differ between the RP and line card, you can ignore this inconsistency because this information is not used during the forwarding process.

  Workaround: Disable the CEF table consistency checker so that no passive scan check is performed of tables of the line cards.

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

- CSCef68439

  Symptoms: The COOL does not trace the RP Up event when the Route Processor (RP) comes back up.

  Conditions: This symptom is observed on a Cisco 12000 series Internet router, which runs Cisco IOS Release 12.0 S.

  Workaround: There is no workaround. Reload the router to clear the condition.

- CSCef69146

  Symptoms: A Cisco 12000 series crashes when the encapsulation of T1 channels is changed to MFR during a cut-and-paste operation of the configuration or when you copy from a file to the running configuration.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S1 and that is configured with a 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card when the configuration is changed at a fast pace. When the configuration lines are entered at a slower pace, the symptom does not occur.

  Workaround: Avoid pasting configuration files to the 1-port channelized OC-12/STM-4 (DS1/E1) ISE line card. If this is not an option, there is no workaround.

- CSCef72305

  Symptoms: A standby PRE crashes on bootup.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 1000 ATM VCs when a forced SSO switchover occurs.

  Workaround: There is no workaround.

- CSCef72411

  Symptoms: Line cards and the standby RP on a Cisco 12000 series may fail when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release for Release 12.0(30)S and that has two PRPs when you enter the **redundancy force-switchover** command. Note that this caveat is resolved in Release 12.0(30)S.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the RP to recover from a Fabric Interface ASIC (FIA) halt condition if this condition occurs following an RP switchover. In a Cisco IOS software release that does not integrate the fix for this caveat, the RP does not attempt to recover from a FIA halt condition after an RP switchover has occurred (but it does attempt to recover from such a conditions in other situations).

- CSCef72555

  Symptoms: When you change the Cisco IOS software image on a Cisco 10000 series, HA may function differently, causing strange behavior, a standby crash, or both.

  Conditions: This symptom is observed when you change the Cisco IOS software image on a Cisco 10000 series from one release train to another release train. This symptom affects Release 12.0S, Release 12.2S, releases that have been derived from Release 12.2 releases, and releases that have been derived from Release 12.3.

  Workaround: There is no workaround.

- CSCef78098

  Symptoms: An Engine 1 or Engine 2 Gigabit Ethernet (GE) line card may stop switching traffic even though the line protocol is up. Pings and routing do not work, and traffic does not go through.

  Conditions: This symptom is observed a Cisco 12000 series after error recovery and when the **negotiation auto** command is not configured for the interface of the GE line card.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface of the line card.

- CSCef80260

  Symptoms: IP packets with an IP length that is smaller than 64 bytes and that have the More Fragments (MF) flag set to 1 do not go through a Cisco 12000 series.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S3 or Release 12.0(28)S1 and that is configured with a 2-port OC-48 DPT Engine 4+ ingress line card.

  Workaround: There is no workaround.

- CSCef80349

  Symptoms: An MPLS traffic engineering (TE) tunnel may not come back up after a link flaps.

Conditions: This symptom is observed when the headend of the TE tunnel is a third-party router that has the **no cspf** command configured for the label switched path (LSP) and when the tunnel midpoint is a Cisco router that runs Cisco IOS Release 12.0(25)S1. The symptom occurs when the link downstream (that is, towards the tailend of the tunnel) on the Cisco router fails because the interface on either side of the link is shut down.

In addition, note that the third-party router does not increment the LSP ID when it receives a message, nor does it send a PathTear message in response to a PathErr message.

Possible Workaround: Use an explicit path on the third-party router but without the **no cspf** command enabled.

- CSCef81555

  Symptoms: The running configuration does not show the correct policing rate if the rate is configured to be larger than 4,200,000,000 bps.

  Conditions: This symptom is observed on a Cisco 12000 series that runs an interim release for Cisco IOS Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCef83864

  Symptoms: A Cisco 10000 series reloads unexpectedly.

  Conditions: This symptom is observed when 750 VRFs are configured.

  Workaround: There is no workaround.

- CSCef86176

  Symptoms: The following CLI commands are missing from a Cisco 12000 series:

```
router(config)#map-class frame-relay r
router(config-map-class)#frame-relay ?
  adaptive-shaping   Adaptive traffic rate adjustment, Default = none
  bc                 Committed burst size (Bc), Default = CIR
  be                 Excess burst size (Be), Default = 0 bits
  cir                Committed Information Rate (CIR), Default = 56000 bps
  custom-queue-list  VC custom queueing
  fecn-adapt         Enable Traffic Shaping reflection of FECN as BECN
  mincir             Minimum acceptable CIR, Default = 1/2 CIR
  priority-group     VC priority queueing
  traffic-rate       VC traffic rate
```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

- CSCef89470

  Symptoms: After you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an active GE interface or after you reload the router while an GE interface is active, the correct ARP entry is missing from the interface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS release later than Release 12.0(23)S.

  Workaround: There is no workaround.

- CSCef89562

  Symptoms: An Engine 4+ EPA-GE/FE-BBRD line card reports "%TX192-3-PAM_MODULE" and "%TX192-3-PAM_PIM" errors, and the interfaces continue to flap with the following error message:

  ```
  %GRPGE-6-INVALID_WORD: Interface GigabitEthernet15/1/0: Detected RX Invalid Word
  ```

  When there is heavy traffic, the line card may crash without generating any crashinfo.

  Conditions: These symptoms are observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S3 or Release 12.0(27)S3.

  Workaround: There is no workaround.

- CSCef90783

  Symptoms: The output counter on the interface of a PE router that faces a P router generates almost twice the value that is should provide.

  Conditions: This symptom is observed in the following MPLS topology in which Cisco 12000 series routers are connected via interfaces of Engine 3 line cards:

  A CE router (CE1) connects to a PE router (PE1) that connects, in turn, to a P router. This P router connects to another PE router (PE2) that, in turn, connects to another CE (CE2) router.

  The symptom occurs when a VRF ping is generated from PE1 to the VRF interface of PE2, that is, the interface that is connected to CE2. The output counter on PE2 generates incorrect values.

  Workaround: There is no workaround.

- CSCef91030

  Symptoms: After the default route is received from a remote PE for a VRF, communication stops for traffic via the default route in this VRF on a Cisco 12000 series that functions as a PE router in an MPLS VPN environment. The packets are switched out of the core MPLS interface untagged as native IPv4 packets instead of with MPLS and BGP labels.

  Conditions: This symptom is observed when the traffic is received from VRF interfaces on an Engine 2 line card that is installed in a Cisco 12000 series that functions as a PE router.

  The symptom occurs in Release 12.0(27)S2, Release 12.0(27)S3, and interim releases for Cisco IOS Release 12.0(30)S. Other releases may be affected too. The symptom does not occur in Release 12.0(24)S2.

  The symptom occurs when the VRF ingress interface is configured on an Engine 2 3-port GE line card or Engine 2 1-port OC-48 POS line card. Other line cards may be affected too. The symptom does not occur when the VRF ingress interface is configured on an Engine 0 4-port OC-3 POS line card or 4-port GE ISE line card.

  Workaround: There is no workaround.

- CSCef91475

  Symptoms: A CPUHOG situation may occur intermittently on a Cisco 12000 series, causing fabric pings to be lost and all OSPF and BGP adjacencies to be dropped.

  Conditions: This symptom is observed in PRP on a Cisco 12000 series router.

  Workaround: There is no workaround. However, the symptom resolves itself.

- CSCef93832

  Symptoms: A router that reboots enters an infinite loop.

  Conditions: This symptom is observed after a router has crashed and when the ROMMON does not gracefully recover during the rebooting process.

Workaround: There is no workaround.

- CSCef94619

  Symptoms: A VIP may crash while forwarding packets or a watchdog timeout crash may occur on the VIP during statistics collection.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RSP4 and that runs Cisco IOS Release 12.0(26)S4.

  Workaround: There is no workaround.

- CSCef96652

  Symptoms: The offered rate counter in the output of the **show policy-map interface** command is inaccurate.

  Conditions: This symptom is observed on a Cisco 12000 series when very high traffic rates are used.

  Workaround: There is no workaround.

- CSCef97536

  Symptoms: When Multiprotocol Label Switching (MPLS) label distribution protocol (LDP) is configured and you enter the **clear ip route** EXEC command, the MPLS forwarding entries for some of the cleared routing prefixes may become unlabeled.

  Conditions: This symptom is observed for prefixes that are connected (with an unspecified nexthop IP address) and that are not locally recognized. This situation may occur in a configuration in which two LDP peers are connected by a point-to-point link that uses PPP encapsulation, and in which both interfaces are configured to use IP addresses with /32 masks.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee12379. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Possible Workaround: Prevent the symptom from occurring by using a shorter network mask when you configure the interfaces or by using another encapsulation such as HDLC.

  When the symptom occurs, restore proper operation by forcing the LDP session that is associated with the link to re-establish itself, or by forcing the LDP session to re-advertise labels for the affected prefixes. The LDP session can be reset by entering the **clear mpls ldp neighbor** command, by administratively disabling and then re-enabling one of the interfaces, or by deconfiguring and then reconfiguring LDP on one of the interfaces. The LDP session can be forced to re-advertise labels by modifying the outbound label filtering configuration. However, this method is complicated and should only be attempted if you are already very familiar with the required procedures, and if the routers do not already have a complicated label filtering configuration in place.

- CSCef97964

  Symptoms: A VIP4-80 crashes when you enter the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco 7513 that runs Cisco IOS Release 12.0(28)S1 and that is configured for SSO.

  Workaround: There is no workaround.

- CSCeg00111

  Symptoms: Padded IP fragments with an IP length that is shorter than 64 bytes and the More Fragments (MF) (which is set to 1) are dropped by an Engine 4+ line card that functions as an egress line card.

Conditions: This symptom is observed when the ingress line card is an Engine 4+ DPT line card and the egress line card is any Engine 4+ line card.

Workaround: There is no workaround.

- CSCeg00252

  Symptoms: When you enter the **show sec-disk0:** command or the **execute-on slot** *slot-number command* command on the standby RP, no command output is generated.

  Conditions: This symptom is observed on a Cisco 12000 series that has dual RPs and that is configured for RPR, RPR+, or SSO redundancy mode. Note that when you enter the **dir sec-disk0:** command on the standby RP, command output is properly generated.

  Workaround: There is no workaround.

- CSCeg00338

  Symptoms: A high CPU utilization may occur at the interrupt level on a Cisco 10000 series when CLNS traffic is forwarded.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with an PRE-1 and that runs Cisco IOS Release 12.0(24)S6.

  Workaround: There is no workaround.

- CSCeg01168

  Symptoms: Counters that are displayed in the output of the **show interface** commands for an ATM interface of an 8-port OC3 ATM line card show incorrect input packet and byte counts.

  Conditions: This symptom is observed on a Cisco 12000 series when the Port Mode Cell Relay Support feature is configured on the ATM interface.

  Workaround: There is no workaround.

- CSCeg01543

  Symptoms: A Cisco 7500 series VIP may crash when its serial interfaces are part of a Multipoint Frame Relay (MFR) bundle.

  Conditions: This symptom is observed when a Frame Relay end-to-end fragment is received on an MFR interface.

  Workaround: Administratively shut down the MFR interface or shut down the MFR interface on the other side of the link.

- CSCeg02511

  Symptoms: A Cisco 10000 series may display %CHSTM1-3-STATESYNC error messages, and a buffer leak may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S2 when a Fast Ethernet interface is configured to use DHCP via the **ip address negotiated** command.

  Workaround: Do not configure the **ip address negotiated** command. Rather, configure a specific IP address.

- CSCeg03055

  Symptoms: Sampled NetFlow may stop functioning.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S3 or a later release and that is configured with an Engine 4 plus 4-port OC-48 line card when the hardware of the line card is reset as a result of an error recovery process.

  Workaround: Disable and re-enable Sampled NetFlow.

- CSCeg03180

  Symptoms: A line card in slot 15 is stuck in the WAITRTRY state.

  Conditions: This symptom is observed on a Cisco 12816 that is configured with dual RPs when an RP switchover followed by a CSC switchover occurs.

  Workaround: Reload the router.

  Alternate Workaround: Power down and power up the router.

- CSCeg06618

  Symptoms: A 6-port channelized T3 line card and a 2-port Channelized OC-3 line card may continuously generate the following error message:

  ```
  %LC_CX3-2-PLIM_CPU_CRASHED: PLIM CPU Tofab755 - plim reset
  ```

  Controllers and interfaces do not recover.

  Conditions: This symptom is observed on a Cisco 12000 series and occurs because of a problem with the recovery mechanism following a forced reset of the PLIM component of the line card. The symptom is visible only if another problem indirectly triggers a forced reset of the PLIM component.

  Workaround: There is no workaround. To recover the affected line card, reload the line card by entering **hw-module slot** *slot-number* **reload** command.

- CSCeg10642

  Symptoms: When six queues are configured on an interface and some of the queues do not have traffic, the bandwidth of those inactive queues should be given to other active queues (queues with traffic) in proportion to their EIR (configured via bandwidth remaining). However, this is not the case. The bandwidth is not proportionally given to all the queues.

  Conditions: This symptom occurs when configuring a policy map that creates six queues in an interface.

  Workaround: There is no workaround.

- CSCeg11421

  Symptoms: A Cisco 10720 crashes when you delete an IPv6 ACL.

  Conditions: This symptom is observed when you delete the IPv6 ACL during the TurboACL compilation.

  Workaround: Wait for the ACL to be fully compiled before you delete it.

- CSCeg13868

  Symptoms: When the **no tag-switching ip propagate-ttl** command is configured on PE routers and a traceroute is executed from one CE router to a remote CE router, an egress PE router replies to the traceroute with the address of its ingress MPLS interface.

  Conditions: This symptom is observed only when the traceroute is destined for a network between an egress PE router and a remote CE router, when the ingress line card of the egress PE router is a Cisco 12000 series Engine 0 or Engine 1 line card.

  Workaround: There is no workaround.

- CSCeg16631

  Symptoms: When you enter the **distribute-list** *interface* command in a global RIP routing context and the interface that is specified in the command is a VRF interface, the command is rejected with the following error message:

  ```
  % The interface is not in the same VRF as the process
  ```

Because the **distribute-list** *interface* command is not implemented in the IPv4 VRF address-family, there is no other way to filter networks received in updates via a VRF interface.

Conditions: This symptom is observed in all Cisco IOS releases that integrate the fix for CSCee32557. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee32557. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: In a configuration that is mentioned above, to filter networks received in updates, enter the **distribute-list** *extended-ACL-reference* command in which the "source-part" of the extended ACL specifies the prefixes and the "destination part" matches on the IP address of the RIP neighbor.

- CSCeg28402

  Symptoms: Spurious memory accesses may occur on a Cisco 7500 series and may cause high CPU usage on the RSP.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed Multilink PPP (dMLP) and that functions in an MPLS network.

  Note that packet switching for MPLS packets over MLP bundles is not supported at the RSP level in Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat causes packets that are sent to the RSP for switching to be dropped. Distributed forwarded packets are forwarded correctly.

- CSCeg30179

  Symptoms: Removing a policy that has shape and bandwidth in the same class (in that same order) may cause a router to crash.

  Conditions: This symptom is observed when the router functions under a traffic load.

  Workaround: There is no workaround.

- CSCin79436

  Symptoms: A Cisco 12000 series does not fragment IP traffic while switching the traffic into the MPLS core even when the size of the incoming IP packets exceeds the IP MTU of the egress interface. This situation causes the traffic to be dropped on the next hop router.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(26)S or a later release when all of the following conditions are present:

  - The traffic leaves through an egress interface of an Engine-3 line card (on the MPLS core side).

  - The imposed label stack contains only explicit null labels.

  - The size of the incoming IP packets exceeds the IP MTU of the egress interface.

  Workaround: Ensure that the IP MTU of the egress interface exceeds the maximum size of the incoming IP packets.

- CSCin79899

  Symptoms: When error recovery is performed on a 3-port Gigabit Ethernet (GE) line card that has port 0 in the shutdown state, the 3-port GE line card stop passing traffic on all ports.

  Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(23)S or a later release and that is configured with an Engine 2 3-port line card.

  Workaround: Reload the 3-port GE line card and leave port 0 in the up/down state.

- CSCin82862

  Symptoms: Multicast traffic is not switched from a multilink interface on a Cisco 7500 series that is configured for distributed multilink PPP (MLP).

  Conditions: This symptom is observed when the router is reloaded or when the multilink interface flaps.

  Workaround: Enter the **clear ip mds linecard *** command on the Route/Switch Processor (RSP).

- CSCin83445

  Symptoms: Incoming multicast traffic on a distributed MLP link is process-switched.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed MLP after the router has been reloaded.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink interface.

- CSCsa46154

  Symptoms: A Route Processor (RP) failover occurred.

  Conditions: This symptom occurred while using the **show route- map** command in one session and removing several route-maps in rapid succession in another session.

  Workaround: Do not use the **show route-map** command while removing route-maps in a concurrent vty session.

Wide-Area Networking

- CSCee75882

  Symptoms: A GEIP+ that is installed in VIP may crash.

  Conditions: This symptom is observed on a Cisco 7500 series when the Gigabit Ethernet interface or the interface of its neighbor flaps.

  Workaround: Stabilize the flapping interface.

- CSCef45502

  Symptoms: A connection remains to exist on a line card even though the connection is deleted on the RP.

  Conditions: This symptom is observed on a Cisco 12000 series when you enter the **no frame-relay interface-dlci** command.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCin05330

  Symptoms: When a multilink bundle interface is created by entering the **interface multilink** *group-name* global configuration command, the Cisco Discovery Protocol (CDP) becomes incorrectly disabled. If the **cdp enable** interface configuration command is used to enable CDP on the multilink bundle interface, the command is not saved in the startup configuration and CDP remains disabled after the router is reloaded.

  Conditions: This symptom is observed on a Cisco platform that is configured with a multilink bundle interface.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(27)S3

Cisco IOS Release 12.0(27)S3 is a rebuild of Cisco IOS Release 12.0(27)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(27)S3 but may be open in previous Cisco IOS releases. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCea21328

  Symptoms: After a Versatile Interface Processor (VIP) has reloaded, there does not seem to be a crashinfo file because the crashinfo file is not closed; therefore, it is not visible or accessible. If the same VIP reloads again, both the first and second crashinfo files are accessible.

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(6f). The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCeb20967

  Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an Symptoms: A Route Switch Processor (RSP) may reload unexpectedly when a bus error with an invalid memory address occurs while packets are placed into a hold queue.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S, 12.1(14)E4, or 12.2 S when the following sequence of events occurs:

  1. A packet is switched via Cisco Express Forwarding (CEF).
  2. The egress interface has queueing/shaping configured.
  3. The egress interface is congested, causing the packet to be placed into the hold queue.

  Workaround: There is no workaround.

- CSCec39376

  Symptoms: A Flash memory card may become corrupted. The output of the **show** *flash-filesystem* EXEC command may display the following information:

  ```
  Open device slot0 failed (Bad device info block)
  ```

  Conditions: This symptom is observed on a Cisco platform when you perform an online insertion and removal (OIR) of the Flash memory card.

  Workaround: Do not perform an OIR of the Flash memory card. Rather, switch off the router and perform an offline insertion and removal.

  If the Flash memory card does become corrupted after an OIR, reformat the Flash memory card.

- CSCec69536

  Symptoms: When you reload a Cisco 7500 series router with a new Cisco IOS software image, the router may reload unexpectedly during the bootup process and generate an “Imprecise cache parity error” message.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Route Switch Processor 8 (RSP8) and that runs Cisco IOS Release 12.0 S or Release 12.2(18)S when you reload the router with an image of Cisco IOS Release 12.3 T.

  Workaround: Do not reload the router. Rather, power-cycle the router to properly load the image of Cisco IOS Release 12.3 T.

- CSCed33110

  Symptoms: A VIP crash may cause memory exhaustion on an RSP, which in turn may cause the RSP to crash.

  Conditions: This symptom is observed more frequently on routers with a high IDB count.

  Workaround: There is no workaround.

- CSCed75238

  Symptoms: A serial interface on a Cisco 7500 series may stop transmitting traffic and may report the following VIP crashes: 1

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.3(5a) but may also occur in other releases. This symptom is not observed in Release 12.1(8c).

  Workaround: There is no workaround.

- CSCed86286

  Symptoms: A router may reload due to a software-forced crash.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.2(13)T5 and that has SSH configured. However, the symptom may occur on other platforms that run other releases and that do not have SSH configured.

  Workaround: There is no workaround.

- CSCee04316

  Symptoms: A TN-2-BADCONN message may appear in the log and may be quickly followed by an FIB Disable message, indicating that distributed CEF is disabled on all VIPs. The IPC buffers usage may grows very large (up to 600 MB) and these buffers may not be reclaimed.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 and that has a very large BGP table and several VRFs.

  Workaround: Reload the router to restore normal operation.

- CSCee35740

  Symptoms: After a VIP crashes, a FIB-3-FIBDISABLE error message due to an IPC timeout may occur for all the slots of the VIP.

  Conditions: This symptom is observed on a Cisco 7500 series after the VIP crashes and before the VIP recovers. The FIB-3-FIBDISABLE error message is generated for all the slots of the VIP, causing dCEF switching to become disabled.

  Workaround: There is no workaround. You can reenable dCEF by entering the **clear cef linecard** command.

- CSCee39972

  Symptoms: A Cisco router may experience a memory leak in the IPC buffers:

  Interface buffer pools: IPC buffers, 4096 bytes (total 41664, permanent 624): 0 in free list (208 min, 2080 max allowed) 3339198 hits, 75195 fallbacks, 0 trims, 41040 created 4254 failures (65497 no memory)

  You can also see that the Pool Manager process is holding onto more and more memory:

  PID TTY Allocated Freed Holding Getbufs Retbufs Process 5 0 246913476 44522964 202605044 176561380 2654280 Pool Manager

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or 12.0(26)S1. The memory leak is triggered by the SNMP polling of specific OIDs within the ciscoEnhancedMemPoolMIB MIB.

Workaround: Prevent the MIB from being polled by explicitly configuring an SNMP view in the Cisco IOS configuration. To prevent this MIB from being accessed via any community strings, create a view and apply the view to all communities configured, such as:

snmp-server view NOMEMPOOL iso included snmp-server view NOMEMPOOL ciscoEnhancedMemPoolMIB excluded snmp-server community public1 view NOMEMPOOL ro 6 snmp-server community public2 view NOMEMPOOL ro 7 snmp-server community public3 view NOMEMPOOL ro 8

The specific MIB that is being blocked is the ciscoEnhancedMemPoolMIB MIB (1.3.6.1.4.1.9.9.221).

Once the configuration is in place, the router must be reloaded to clear the IPC cache and free the memory.

- CSCee78266

  Symptoms: A Cisco 7500 series may reload in an indefinite loop when you unintentionally enter the **show list** *number* hidden command.

  Conditions: This symptom is observed when you, for example, abbreviate the **show line 2000** command as the **show li 2000** command and actually execute the **show list 2000** hidden command.

  Workaround: Do not abbreviate the **show line** command as the **show li** command but enter the full command.

- CSCin44135

  Symptoms: A slave RSP running in HSA mode may crash with a cache parity exception.

  Conditions: This symptom is observed on a Cisco 7500 series and occurs only when the slave RSP is an RSP8 or RSP16 that runs in HSA mode.

  Workaround: There is no workaround.

  The fix for this caveat turns off the L3 cache by default on an RSP8 or RSP16 that functions as a slave and that runs in HSA mode; you do not need to do anything specific to turn off L3 cache by default on an RSP8 or RSP16 that functions as a slave and that runs in HSA mode.

  For an RSP8 or RSP16 that functions as a slave and that runs in a non-HSA mode such as RPR, you can turn off the L3 cache by entering the **l3 cache bypass** command on the master RSP while the slave RSP8 or RSP16 still runs in a non-HSA mode.

  Because the slave RSP performs non-CPU intensive operations, regardless of the mode of operation, turning off the L3 cache does not have any undesirable impact.

Interfaces and Bridging

- CSCec15909

  Symptoms: In a High Availability (HA) environment with Stateful Switchover (SSO) enabled and while trying to configure framing for T1 on T3 PA, the standby route processor (RP) gets reloaded giving a “CCB playback failed” error.

  Conditions: The defect is seen with SSO or RPR-Plus enabled on T3 family of port adaptors. The trigger is the change in framing configuration for T1 on T3 PA.

  Workaround: Administratively shutdown all interfaces on T1 before changing the framing.

- CSCee47714

  Symptoms: Entering the **shutdown** command on a controller of a Packet over T1/E1 Network Transceiver puts the controller permanently down. Entering the **no shutdown** command on the controller does not bring the controller up.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S and is specific to the controller that is installed in a PA-MC-8T1/E1, PA-MC-4T1/E1, or PA-MC-2T1/E1 port adapter.

  Workaround: There is no workaround.

- CSCin66616

  Symptoms: The output of an snmpwalk for the entPhysicalDescr MIB on a PA-MC-8E1/120 may shows the PA-MC-8E1/120 as unknown.

  Conditions: This symptom is observed on a Cisco 7500 series in which a PA-MC-8E1/120 in installed.

  Workaround: There is no workaround.

- CSCin67296

  Symptoms: Channelized interfaces on a channelized T3 line card or port adapter that is configured for Frame Relay encapsulation may be in the up/down state, and DLCIs are inactive.

  Conditions: This symptom is observed when you reload a Cisco platform and when the interfaces were in the up/up state before you reloaded the platform.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller of either the T3 line card or port adapter on the Cisco platform or on the T3 line card or port adapter on the platform at the remote end.

  Alternate Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the main interface on the Cisco platform.

IP Routing Protocols

- CSCec22723

  Symptoms: A router may unexpectedly reload from a watchdog timeout in OSPF.

  Conditions: This occurs when using OSPF routing protocol and enabling **iSPF**

  Workaround: Remove iSPF configuration from OSPF by issuing **no iSPF**

- CSCec55418

  Symptoms: A Cisco router may reload unexpectedly at “ospf_area_delete().”

  Conditions: This symptom is observed on a router that is configured for Open Shortest Path First (OSPF) when all of the following conditions are present:

  - A large number of **network** commands are removed from the configuration at once via a cut-and-paste operation.

  - All of the **network** commands for an area are removed.

  - A **no area** command is entered for an area that is referenced in the **network** commands.

  Workaround: Do not use a cut-and-paste operation to remove the **network** commands simultaneously with the area that is referenced in the **network** commands.

- CSCed53358

  Symptoms: Pings fail on an Ethernet-to-VLAN interworking over L2TPv3 due to an IRDP failure.

  Conditions: This symptom is observed when you ping between two CE routers. Both of the CE routers do not learn each other's MAC address automatically.

  Workaround: Ping from the first CE router to the second CE router, then ping from the second CE router to the first CE router.

- CSCed57403

  Symptoms: When a Cisco router is a midpoint of a TE tunnel and the tunnel headend is a third- party vendor router, the Cisco router may crash.

  Conditions: This symptom is observed during a period of network instability and may occur when a TE tunnel does not contain an EXPLICIT ROUTE object and when the tunnel is dynamically routed by using OSPF cost only.

  Workaround: Use an EXPLICIT ROUTE object or ensure that there are no alternate paths in the network.

- CSCed60800

  Symptoms: The withdraw message of a multipath (not bestpath) from a BGP neighbor deletes the path from the BGP table but it does not uninstall the route from the IP routing table.

  Conditions: This symptom is observed when the **maximum-paths eibgp** command or **maximum-paths ibgp** command is configured.

  Workaround: Enter the **clear ip bgp *** or disable the **maximum-paths eibgp** command or **maximum-paths ibgp** command.

  Alternate Workaround: if the number of possible EBGP peers are less or equal to 2 then the problem is transient and not obviously noticeable.

- CSCed86069

  Symptoms: A software-forced chunk corruption crash may occur when a MALLOC failure occurs.

  Conditions: This symptom is observed on a Cisco platform that has the **bgp dampening** command enabled.

  Workaround: There is no workaround.

- CSCed93630

  Symptoms: A Cisco router may reload unexpectedly when a **bgp debug** command is enabled.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, 12.2S, or 12.3T.

  Workaround: There is no workaround.

- CSCee24899

  Symptoms: A router that is configured for multicast routing may reload due to a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software release that contains the fix for CSCec80252. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec80252. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCee36721

  Symptoms: An OSPF Designated Router (DR) may fail to regenerate the network LSA when you reload the router.

  Conditions: This symptom is observed on a Cisco router that functions as a DR for an OSPF interface when another interface with the same interface address is present in the area but is in a shut down state.

  Workaround: Remove the duplicate interface address and enter the **clear ip ospf process** command.

- CSCee40207

  Symptoms: The BGP Open processes may hold more and more memory, may cause a memory leak, may finally run out of memory, and may cause a Malloc Failure error.

  Conditions: This symptom is observed when there are BGP neighbors stuck in the active state (that is, a BGP neighbor is configured but the peer address is not reachable) and when some NSF/SSO RP switchovers occur and the standby becomes active.

  Workaround: Shut down the neighbors that are not used.

  Further Problem Description: When the memory leak occurs, 1 Kb of memory leaks every two minutes for each BGP neighbor that is not up.

- CSCee41172

  Symptoms: The **maximum-paths import** *number-of-paths* command enables a VRF to import additional paths in addition to the bestpath. If the original path of the import path is withdrawn, wrong import paths may be purged. This situation may cause traffic disruption up to 15 seconds.

  Conditions: This symptom is observed when the original path of the best import path is withdrawn and the import path is at the end of the path list (that is, the one learned the very first). In this situation, all import paths that are derived from other paths may be purged as well. If the imported net has only import paths, the net may not be reachable until other paths are reimported.

  Workaround: Ensure that the import path is at the top of the path list or use the same route descriptor (RD) for all import paths.

- CSCee59315

  Symptoms: A BGP VPNv4 table may contain paths that may be imported from deleted BGP table entries or from table entries that have a different prefix from the importing prefix.

  An example of a path from a deleted BGP table entry is as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
BGP routing table entry for 200:2:192.168.0.0/32, version 52
Paths: (1 available, best #1, table vpn2)
  Advertised to non peer-group peers:
  10.4.1.2
  2 100, imported path from 2829:2829:185404173:11.13.11.13/-53
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:3
```

  The entry that this path is imported from has been removed from the table and its memory contents contain an incorrect pattern. When the incorrect pattern is displayed as a prefix, it appear as “2829:2829:185404173:11.13.11.13/-53”.

  A mismatched prefix appears as follows:

```
Router# sh ip bgp v v vpn2 192.168.0.0
```

```
BGP routing table entry for 200:2:192.168.0.0/32, version 54
Paths: (2 available, best #1, table vpn2)
Flag: 0x820
  Advertised to non peer-group peers:
  10.10.10.10 10.20.20.20
  2
    10.4.1.2 from 10.4.1.2 (10.4.1.2)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: RT:1:2
  2 100, imported path from 200:2:172.16.0.0/24
    10.1.1.2 from 10.1.1.2 (10.1.1.2)
      Origin IGP, localpref 100, valid, external
      Extended Community: RT:1:3
```

This BGP VPNv4 table entry is for prefix 192.168.0.0/32 but it shows that a path is imported from 172.16.0.0/24. This situation occurs when a path has a link to a deleted BGP table entry, and then the memory for the deleted entry is reused for a new table entry of which the prefix may not match with the importing entry.

Conditions: These symptoms are observed when you enter the **maximum-paths import** *number* command in router BGP address-family IPv4 VRF mode. The *number* argument indicates the number of paths to import from one VRF to another.

Workaround: Remove the **maximum-paths import** *number* command from the router BGP address-family IPv4 VRF mode.

- CSCee69396

  Symptoms: A Cisco 10000 series router that is running Cisco IOS Release 12.0(25)SX6 notices a large increase of at least 15% in the CPU usage in the “BGP Router” process when upgraded from Cisco IOS Release 12.0(23)SX5. This occurs under certain conditions where there are a very large number of BGP neighbors in a PE-CE scenario. During the steady state after BGP router convergence, there needs to be a constant churn in the updates with addition/withdrawal of the routes from the neighbor BGP peers.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.0(25)SX6. All versions starting from Cisco IOS Release 12.0(25)SX to Release 12.0(25)SX6 are affected by this problem.

  Workaround: Configure the neighbors by grouping into sets or peer-groups, in which a few of the neighbors in each set share similar outbound policy. Each set will fall into a separate update group or peergroup.

- CSCee83549

  Symptoms: When multipath is configured, one of the paths may have an inconsistent (old) label, causing only one path to be operational.

  Conditions: This symptom is observed when BGP does not update the outlabel information in the TFIB and for CEF.

  Workaround: Clear or readvertise the route that is inoperational.

- CSCee89438

  Symptoms: An MSDP enabled RP does not build an (S,G) state from its SA cache when it should do so. Depending on the topology and if an SPT threshold is configured as infinite, this situation may result in a multicast forwarding interruption of up to 2 minutes.

Conditions: This symptom is observed when the RP for a group fails and an incoming (*,G) join message is received.

MSDP should create an (S,G) state from its SA cache. However, this is done before the (*,G) olist is populated; because of the (*,G) NULL olist, MSDP does not install an (S,G) state.

Workaround: Enter the **clear ip mroute *** command on all first-hop routers to the source to enable the FHR to register immediately when the next packet creates an (S,G) state.

- CSCef00535

  Symptoms: An OSPF router may reload unexpectedly.

  Conditions: This symptom is observed after a neighbor has performed a switchover.

  Workaround: Disable LLS under the OSPF process on the router by entering the **no capability LLS** command or disable OSPF NSF under the OSPF process on the neighbor by entering the **no nsf** command.

- CSCef17311

  Symptoms: An %ALIGN-3-SPURIOUS error message and a traceback may be generated when you configure BGP and MPLS VPN.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(9.10)T but may also occur in other releases such as Release 12.0 S and Release 12.2 S.

  Workaround: There is no workaround

- CSCin65241

  Symptoms: ISIS redistribute commands are not synced to the standby RP. The routes dependent on these commands will fail after switchover.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

Miscellaneous

- CSCea65827

  Symptoms: A Cisco router performing MPLS label imposition on IPv4 traffic may reload.

  Conditions: This symptom is observed when the router attempts to forward traffic to a destination via a route that is newly learned, when the router forwards traffic via Cisco IOS software (that is, not via hardware acceleration), and when one of the following conditions is present:

  - There are multiple routes to the destination.
  - The **ip cef accounting non-recursive** command is enabled.
  - CEF does not install a “cached adjacency” (as seen in the output of the **show ip cef** *prefix* command.)

  The symptom affects the following Cisco IOS releases:

  - Releases later than Cisco IOS Release 12.0(22)S.
  - Cisco IOS Release 12.1 T and a special XT-release that is based on Cisco IOS Release 12.1 T.
  - Release earlier than Cisco IOS Release 12.2 S.
  - Releases later than Cisco IOS Release 12.2(2)T.
  - Cisco IOS Release 12.3.

  The symptom does not affect the following Cisco IOS releases:

  - Cisco IOS Release 12.1E
  - Cisco IOS Release 12.2M

  Workaround: Avoid conditions that prevent a "valid cached adjacency" from being installed.

- CSCec11645

  Symptoms: VIP crashes with DMA Receive error.

  Conditions: This symptom can occur when doing xconnect hairpinning of two interfaces on the same VIP.

  Workaround: There is no workaround.

- CSCec15517

  Symptoms: A Cisco router may reload when you enter the **show policy-map interface** command in one router session while deleting the sub-interface on which the policy is attached from another session.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Frame Relay permanent virtual circuit (PVC) policy.

  Workaround: There is no workaround.

- CSCec82589

  Symptoms: After entering a **no hw-module slot** command on the primary CSC, an Engine 0 OC-12 (channelized to DS3) line card may be come inoperable.

  Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(24)S.

  Workaround: Use the **microcode reload** global configuration command to reload the line card.

- CSCed02844

  Symptoms: IPv6 adjacencies may appear as incomplete, and connectivity may be broken. This situation occurs at random times and is not associated with any event in particular. IPv4 adjacencies may appear as incomplete but recover within a minute.

  Conditions: This symptom is observed on a Cisco IOS-based router when you enter the **clear adjacency** command.

  Workaround: To restore the correct state of the adjacency, enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed41231

  Symptoms: An alignment error may cause a Cisco router to reload unexpectedly.

  Conditions: This symptom is observed under rare conditions (an "extreme corner case") on a MIPS-based Cisco platform or on a Versatile Interface Processor (VIP), port adapter, or line card that contains a MIPS processor. The symptom is not release-dependent and may occur in all Cisco IOS releases.

  Workaround: There is no workaround.

  Further Problem Description: All Cisco 7500 VIPs and Cisco 7200 NPEs use MIPS- based processors. The following are additional platforms that use MIPS processors:

  Cisco 2691, Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 4500, Cisco 4500-M, Cisco 4700, Cisco 4700-M, Cisco AS5300, Cisco AS5400, Cisco AS5450, Cisco AS5800 router shelf, Cisco AS5800 system controller (3640 based), Cisco 7120, Cisco 7140, Cisco

UBR7100, Cisco UBR7200 - all NPEs, Cisco 7301, Cisco 7304, Cisco 7400, Cisco 6500 MSFC, Cisco 6500 MSFC2, Cisco 7600 MSFC, Cisco 7600 MSFC2, Cisco 10000, Cisco UBR10012, Cisco 12000 GRP, Cisco and most (if not all) 12000 line cards.

- CSCed62835

  Symptoms: A Cisco platform may crash after the following error is seen:

  SCHED: Stack for process CEF IPC Background running low, 48/6000 %SYS-SP-6-STACKLOW: Stack for process CEF IPC Background running low, 48/6000

  Conditions: This symptom is observed with a recursive prefix with multiple next hops when these next hops match host routes that themselves are recursive prefixes and recurse through themselves.

  Workaround: Avoid recursion loops.

- CSCed63357

  This caveat consists, of six separate symptoms, conditions, and workaround, of which the first three apply to all Cisco IOS releases and the last three apply only to Cisco IOS Release 12.3 T:

  1) Symptoms: There are three symptoms:

  – There may be a inconsistent or duplicate display of files between the **show disk***slot-number* and **dir disk***slot-number* commands.
  – When a file is deleted from the CLI, the file may be deleted but a “No such file” message may be printed.
  – One cluster may leak. Entering the **fsck** command truncates the original file and creates an orphan file for the leaked cluster.

  Conditions: This symptom is observed when an application creates or opens a file without the “O_TRUNC:” mode, as in the following example:

```
show version | append disk#:

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#vtp file new
Setting device to store VLAN database at filename new.
Router(config)#^Z
```

  Workaround: There is no workaround.

  2) Symptoms: The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information (such as inconsistent file sizes) when multiple images are copied.

  Conditions: This symptom is observed when you make two copies of the image file to the disk by using two vtys and by entering the **dir disk***slot-number* command at the same time.

  Workaround: Do not enter the **show disk***slot-number* and **dir disk***slot-number* commands when multiple images are being copied.

  3) Symptoms: There are two symptoms:

  – The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
  – Entering the **fsck** command may delete or truncate the valid files or create an orphan file for an unused cluster.

  Conditions: This symptom is observed when you rename a directory that consists of many subdirectories or files.

  Workaround: Reload the router.

4) Symptoms: There are two symptoms:

- There may be a duplicate entry for each file when you enter the **show disk***slot-number* command.
- An snmpGet on a ciscoFlashFileSize object may enter a loop.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T after the router boots up.

Workaround: There is no workaround.

5) Symptoms: There are two symptoms:

- The **show disk***slot-number* and **dir disk***slot-number* commands may show inconsistent information.
- Entering the **fsck** command may delete or truncate the original file.

Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3 T when an application or a CLI command overwrites a file on the disk.

Workaround: Reload the router.

6) Symptoms: A router that runs Cisco IOS Release 12.3 T crashes.

Conditions: This symptom is observed when an application creates or opens a file without the "O_TRUNC" mode and attempts to delete the file, as in the following example:

```
show version | append disk0:redirect.out" and issuing
delete disk0:disk0:redirect.out
```

Workaround: Reload the router and delete the file.

- CSCed63508

  Symptoms: Up to 10 percent of packets that are larger than 1496 bytes are dropped when passing through an Engine 3 4-port GE line card (4GE-SFP-LC).

  Conditions: This symptom is observed on a Cisco 12000 series when the line card is used for both the ingress and egress traffic flow. This situation occurs when SNF is configured on the egress interface of the affected line card by entering the **ip route-cache flow sampled output** command.

  Workaround: Increase the MTU on any interface of the Engine 4-port GE line card to 1530 bytes to enable the buffer resources of the line card to be initialized with a larger size.

  Alternate Workaround: Decrease the rate of packets drops by increasing the sampling period. For example, when you enter the **ip flow-sampling-mode packet-interval 10** command, up to 10 percent of packets that are larger than 1496 bytes are dropped. However, when you enter the **ip flow-sampling-mode packet-interval 1000** command, only 0.1 percent of packets that are larger than 1496 bytes are dropped.

- CSCed64702

  Symptoms: On a Cisco 10000 series, the PXF information may not be correctly updated from the RP after a route change, causing packets to be sent untagged even though the RP shows that the packets should be sent as tagged.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(26)S.

  Workaround: Enter the **clear isis *** command or enter the **shutdown** command followed by the **no shutdown** command on the interface towards the MPLS cloud.

- CSCed69546

  Symptoms: When mixed channels are defined on a channelized OC-12 line card and these channels include DS3s, T1s, an DS0s, CEF/RIB inconsistency may occur, preventing traffic to be sent over the correct interfaces.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: When you delete interfaces or subinterfaces on the channelized OC-12 line card, ensure that the adjacency for the deleted interface is deleted before you configuring a new interface.

  This can be checked by entering the **show adjacency** or **show adjacency | include** *interface name* command. When the adjacency no longer appears in the output of the **show adjacency command, it is safe to add new interfaces.**

  Note that the **show adjacency** *type number* command cannot be used to get the required information.

  When deleting large numbers of interfaces, a delay of about 2 minutes should be enough to ensure that all of the adjacencies have been deleted.

- CSCed69856

  Symptoms: A Cisco 10000 series router may crash when access control lists (ACLs) are displayed.

  Conditions: The symptom is observed when ACLS are displayed by entering the **show access-list** command just after an ACL has been added, deleted or modified. The probability of the crash increases with the size of the ACL and with the number of times it is used (for example, in route maps).

  Workaround: Wait for a few minutes after modifying the ACL. For large size ACLs (with hundreds of entries) that is used many times you may have to wait between 5 and 10 minutes.

- CSCed74933

  Symptoms: A Cisco 12000 series may exhibit high CPU utilization in the “Per-Second Job” process.

  Conditions: This symptom is observed on a Cisco 12012 router that has a GRP and that is running Cisco IOS Release 12.0(26)S1 with 255 class maps applied to a 4-port ISE Gigabit Ethernet line card. However, the symptom is release- and platform-independent.

  Workaround: Reduce the number of applied class maps.

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

  Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

  Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- CSCed79218

  Symptoms: A Cisco 7200 series router with a PA-2CT3+ or PA-CT3 port adapter does not provide the configured minimum bandwidth guarantees.

  Conditions: This behavior appears to be limited to the multichannel T3 family of port adapters and appears consistently upon the configuration of CBWFQ.

  Workaround: There is no workaround.

- CSCed82592

  Symptoms: A PXF engine on a Cisco 10000 series may unexpectedly crash and then the router may crash.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(23)S5.

  Workaround: There is no workaround.

- CSCed92837

  Symptoms: After a Stateful Switchover (SSO) occurs on a Cisco 7500 series, the standby Route Switch Processor (RSP) my hang just before downloading the image. This situation may prevent the router from entering the STANDBY-HOT state and from being capable to perform a switchover until the standby RSP is reset.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0 S or 12.2 S and that is configured for SSO/Nonstop Forwarding (NSF).

  Workaround: There is no workaround. After the problem occurs, you can recover the router by either waiting for an IPC timer to expire (the default time is 30 minutes) or by entering the **hw-module sec-cpu reset** command.

- CSCed95753

  Symptoms: A GRE tunnel may not work on a PE router.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(25)S or a later release.

  Workaround: There is no workaround.

- CSCee06794

  Symptoms: DTS may not work properly on dot1q Fast Ethernet subinterfaces. Traffic is not shaped at the expected rate

  Conditions: This problem is observed on a Cisco 7500 series that is configured as a PE router and that runs Cisco IOS Release 12.2(12i). The symptom may also occur in other releases.

  Workaround: If this is an option, use ISL subinterfaces.

- CSCee12235

  Symptoms: A Cisco platform reloads because of a watchdog timer expiration.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(20)S2 or Release 12.3 under the following conditions:

  - A service policy (“A”) is attached to an ATM PVC.

  - Policy-map “A” is renamed to “B”.

  - Service policy “B” is attached to the ATM PVC.

  Workaround: First detach the service policy from the PVC, then rename it and attach it again.

- CSCee13932

  Symptoms: Cisco target FEC stack TLVs may not interoperate with those of third-party vendors.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.0(27)S or Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCee14817

  Symptoms: HSRP over the VRF is not working after following these steps:

  1. PE router 1 is the active HSRP router and a redundancy forced switchover occurs on PE router 2 (standby HSRP VPN) with SSO configured.
  2. You enter the **shutdown** command on the GE subinterface of PE router 1.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S3, that has a PRP and 4-port GE ISE line cards, and that functions as a PE router.

  Workaround: Enter the **standby use-bia** command or use RPR+ instead of SSO.

- CSCee14840

  Symptoms: A Cisco 12000 series running Cisco IOS Release 12.0(26)S1 may advertise erroneous IPv6 networks when configured for both 6PE and Route Reflector operation.

  Conditions: This symptom is observed on a network in which 6PE is implemented on an existing dual-stack (IPv4 and IPv6) configuration.

  Workaround: There is no workaround.

- CSCee18889

  Symptoms: If link bundling is configured on any line card in the router and the link bundle is loaded onto an Engine 2 line card that has VPN on FR subinterfaces and that is processing traffic, the Engine 2 line card may reload.

  Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCee22450

  Symptoms: A subinterface on a Cisco 10000 series may drop packets because of unicast RPF check failures, even though the interface is not configured with uRPF.

  Conditions: This symptom is observed on an ATM interface with several subinterfaces when there is at least one subinterface that has uRPF configured. Disabling uRPF on the subinterface still leaves uRPF enabled, even though the CLI indicates it is not enabled. This may also occur with Frame Relay subinterfaces.

  Workaround: Select a subinterface that has uRPF configured, then deconfigure and reconfigure it. This updates all subinterfaces on the interface in such a way that uRPF is correctly enabled or disabled.

- CSCee22810

  Symptoms: On a Cisco 7500 series, all PVCs may suddenly enter the down state and remain in this state for about two minutes before they come back up. During the DLCI down state, the subinterface does not go down and no notifications are observed in the message log.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RPS4+ or an RSP8 and that runs the rsp-jsv-mz image of Cisco IOS Release 12.2(12i). In addition, the router is configured with an 8-port serial port adapter and an HSSI port adapter, is configured for Frame Relay, and has more than 450 PVCs/DLCIs. Note that the symptom may be platform-independent and may also occur on other Cisco platforms in a similar configuration.

  Workaround: There is no workaround.

- CSCee24349

  Symptoms: A Cisco 7500 series cannot boot when there are more than 256 different policy maps attached as service policies on the router.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 but may also occur in Release 12.2 S.

  Workaround: Do not use more than 256 service policies.

- CSCee25588

  Symptoms: A 12000 series Engine 2 line card may not accept a “tx-cos” configuration.

  Conditions: This symptom is observed if the router previously had an Engine 4+ line card in the same slot and this Engine 4+ line card was configured with an output service policy.

  Workaround: Reload the router.

- CSCee27396

  Symptoms: High CPU usage of greater than 90 percent occurs in the CEF Scanner process on all line cards and TFIB-7-SCANSABORTED errors occur when you configure a link bundle.

  Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(26)S1 when the bundle is configured on interfaces gig2/2 and gig6/2. (A 4-port Gigabit Ethernet ISE line card is installed in slot 2 and slot 6.) The link bundle terminates on a third-party vendor switch.

  Workaround: Remove the link bundle and use only one of the Gigabit Ethernet ports.

- CSCee28332

  Symptoms: Multilink MLP in PE may fail / rejected eventually after 3 or more times reloading the CE sides with different IOS images.

  Conditions: The symptom is observed after 3 or more times reloading the CE router.

  Workaround: Create new multilink interface or reload the vip for the bundled physical interface.

- CSCee28481

  Symptoms: After working fine for sometime, a 4-port OC-12 ATM line card stops forwarding unicast packets to the RP, and none of the unicast traffic that is sourced from or destined to the RP via the 4-port OC-12 ATM line card goes through. Unicast traffic to the 4-port OC-12 ATM line card interfaces fails too.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(21)ST7 when MPLS is enabled on the line card. IP traffic and IS-IS traffic that pass through the router are not affected. To recover the line card, reset the line card.

  Workaround: There is no workaround.

- CSCee30527

  Symptoms: After reloading a Cisco 12000 series, the following message may be seen on an Engine 2 or Engine 3 line card:

  ```
  %MBUS-2-DNLDFAIL: IOS download to slot 7 fail, timeout
  ```

  In some cases it may result in LC not coming up:

  ```
  %GRP-3-ABANDON_DOWNLOAD: End attempt to start the linecard in slot 7
  ```

  Conditions: This symptom is observed rarely on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: The line card may come up when you reload the router again.

- CSCee31618

  Symptoms: Buffer leakage could occur when a high load of traffic is sent to an interface that has a service policy enabled. This could result in ping failures or very long packet delay.

  Conditions: The problem is observed with an MC-T3+ interface that is configured in unchannelized mode, and the traffic consists only of small packets such a 64-byte packets.

  Workaround: Manually configure the **tx-ring-limit** command to lower the number of packets that can be placed on the transmission ring.

- CSCee32208

  Symptoms: After a circuit bounces, traffic stops being passed on a VC when using a VC bundle. Other VCs on the same subinterface still work. The switch on the other side of the VC does not show any received cells from the VC.

  In addition, the **show atm vc** command does not work because even after the VC is recovered, the command output still does not show any traffic.

  Conditions: These symptoms are observed on a Cisco 12000 series.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected subinterface.

- CSCee32484

  Symptoms: After performing a manual switchover on a dual-RP router that functions in RPR+ or SSO mode, the following error message may be seen on an 8xOC3ATM line card, and the line card may stop forwarding traffic:

  ```
  %QM-4-STUCK: Port 0 Queue mask 0x80
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of Cisco IOS Release 12.0(28)S.

  Workaround: Perform a microcode reload on the line card.

- CSCee34474

  Symptoms: OSPF peers are mapped to the wrong sub-interfaces.

  Conditions: This symptom occurs after a HA switch over the ATM interfaces were up and appear to be operational with OSPF adjacencies formed.

  Workaround: There is no workaround.

- CSCee36050

  Symptoms: A VIP crashes with the following error message:

  ```
  VIP-3-SYSTEM_EXCEPTION: VIP System Exception occurred sig=10, code=0x10
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when you re-use a channel group (or subinterface) that was previously configured with a Frame Relay DLCI “set” service policy.

  Workaround: Remove the “set” service-policy before you remove the channel group (or subinterface).

- CSCee38324

  Symptoms: A VIP may crash.

  Conditions: This symptom is observed on a Cisco 7500 series when QoS is configured on the interface of the VIP and traffic is flowing.

  Workaround: There is no workaround.

- CSCee38348

  Symptoms: The SNMP counters and CLI for Frame Relay subinterfaces may be incorrect.

  Conditions: This symptom is observed a Cisco 12000 series with ISE POS line cards.

  Workaround: There is no workaround.

- CSCee38942

  Symptoms: EoMPLS tunnels do not have labels assigned to them, preventing a virtual circuit from coming up.

  Conditions: This symptom is observed when multiple (for example, 1200) EoMPLS tunnels are configured. Only on a few tunnels the symptom may not occur.

  Workaround: There is no workaround.

- CSCee39853

  Symptoms: A Cisco router that is running Cisco IOS Release 12.0(25)SX1 may experience CEF disabling on standby PRE.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(25)SX1. The symptom may also occur in Release 12.0 S.

  Workaround: Reset standby PRE.

- CSCee39854

  Symptoms: A ping or Telnet connection to a connected CE router may fail from a Cisco 12000 series router that functions as a PE router.

  Conditions: This symptom is observed on Cisco 12012 that runs Cisco IOS Release 12.0(21)ST3 or a later release when the router has a 3-port Gigabit Ethernet line card that is configured for dot1q encapsulation on its subinterfaces.

  This symptom occurs because of a misconfiguration on the subinterfaces: when you configure a subinterface with new a VRF without removing the already configured VRF, the symptom occurs.

  Workaround: Unconfigure and reconfigure the VRF configuration on the misconfigured subinterfaces.

- CSCee42279

  Symptoms: During an L2TPv3 test with a Cisco 12000 series 4-port OC-12 ATM line card, when you bump traffic on more than two ports that process a high rate of traffic, traffic may stop. When this situation occurs, the CPK24 FPGA on the line card generates ingress packet length errors and sometimes SDRAM CRC errors.

  Conditions: This symptom is observed on a 4-port OC-12 ATM line card that is configured for L2TPv3 and that is installed in a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0 S.

  Workaround: Reload the line card.

- CSCee43562

  Symptoms: The feature manager queue on the Route Processor may not drain for 20 minutes after a reload in a scaled environment with 1400 IP and L3VPN connections (subinterfaces). The feature manager pushes ACL and PBR configurations to the IP Services Engine (ISE) line cards for TCAM processing. You can monitor the state of the feature manager queue with the **show fm queue** command.

  Conditions: This symptom is observed on a 12000 series that runs Cisco IOS Release 12.0(28)S and may occur on any ISE line card that uses an associate message in the QoS manager.

Workaround: There is no workaround.

- CSCee43569

  Symptoms: The TE DB on a tunnel headend may become corrupted.

  Conditions: This symptom is observed on a Cisco router that has MPLS configured.

  Workaround: There is no workaround.

- CSCee43880

  Symptoms: After reloading an E2 16-port OC-3 POS line card that is a member line card of POS channel, the peer POS channel members do not become active members again.

  Conditions: The symptom is observed on a link-bundling interface of a Cisco 12000 series router that runs Cisco IOS Release 12.0 S.

  Workaround: There is no workaround.

- CSCee45099

  Symptoms: A Cisco 12000 series 8-port OC-48 or 2-port OC-192 line card may crash.

  Conditions: This symptom is observed when the line card is configured for MPLS-TE FRR.

  Workaround: There is no workaround.

- CSCee51126

  Symptoms: A Cisco 12000 series may drop 2 to 3 percent of the ping packets that are destined to the router when the input interface is an Engine 4+ line card.

  Conditions: This symptom is observed for ICMP packets on a Cisco 12000 series that is Cisco IOS Release 12.0(26)S1. The symptom may also affect other types of packets.

  Workaround: There is no workaround.

- CSCee51725

  Symptoms: A Cisco 7200 or Cisco 7500 series is reloading after a few minutes of uptime because of a Software Forced Crash.

  Conditions: This is observed on a router running Cisco IOS Release 12.0(27)S1, with a Gigabit Ethernet port adapter or GEIP/GEIP+, if 16 or more HSRP groups are configured.

  Workaround: Reducing the number of HSRP groups to 15 or less will prevent the reloads.

- CSCee54143

  Symptoms: An E1 port on a PA-MC-8T1 port adapter may stay down after a VIP crash.

  Conditions: This symptom is observed on a Cisco 7513 that is configured with a VIP in which a PA-MC-8T1 port adapter with a channelized E1 (or T1) port is installed in slot 0.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCee54198

  Symptoms: A Cisco 12000 series crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco 12016 that runs Cisco IOS Software 12.0(25)S2 when you enter the **hw-module slot 17 shutdown** command to shut down the master scheduler card.

  Workaround: Do not shut down the master scheduler card.

- CSCee57485

  Symptoms: There are two symptoms:

  – Packets with explicit null labels may be dropped from an Engine 4+ POS line card.

  – CEF may become disabled on an Engine 4+ POS line card.

  Conditions: These symptoms are observed on a Cisco 12000 series under the following conditions:

  – The router functions as a PE router with the Engine 4+ POS line card facing the core and performing MPLS disposition.

  – VRFs are configured on the router.

  – The Explicit Null feature is enabled on the router.

  Workaround: There is no workaround.

- CSCee58770

  Symptoms: A Cisco router may generate the following error message:

  ```
  %TUN-5-RECURDOWN: Tunnel2 temporarily disabled due to recursive routing
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2 and that is configured with a tunnel services card (TSC) (that is, a 1-port OC-48 POS line card) when MPLS TE tunnels are configured on the router and when static routes are added.

  Workaround: There is no workaround.

- CSCee59106

  Symptoms: The performance of an OC-48 to E3 concatenated or channelized line card may drop from 4 Mpps to 2.84 Mpps when oCAR is enabled in a configuration that includes both the **conform-action** and **exceed-action** keywords and when oCAR is transmitting packets and changing the precedence.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the c12kprp-p-mz image of Cisco IOS Release 12.0(28)S or an earlier release. However, note that performance drops do not occur in Release 12.0(27)S1.

  Workaround: There is no workaround.

- CSCee59585

  Symptoms: On a Cisco router, the output of the **execute-on slot** *number* **show ip cef** *prefix* command may display the same imposed label twice for a recursive public route.

  Conditions: This symptom is observed on a Cisco platform that supports distributed forwarding such as a Cisco 7500 series or a Cisco 12000 series when the **neighbor** *name* **send-label** command is configured under an IPv4 BGP address family on a VIP or line card and when one of the following actions occurs:

  – You enter the **clear cef linecard** command.

  – You perform an OIR of the VIP or line card.

  – You enter the **no ip cef distributed** command followed by the **ip cef distributed** command.

  The symptom disappears after the affected prefix flaps.

  Workaround: There is no non-impacting workaround, but you can enter the **clear ip route** *prefix* command or reset the BGP peer to solve the problem.

- CSCee63939

  Symptoms: An Engine 6 line card may crash during the MDFS process.

Conditions: This symptom is observed on a Cisco 12000 series when multicast and unicast traffic are running through the Engine 6 line card.

Workaround: There is no workaround.

- CSCee65004

  Symptoms: A 1-port 10-Gigabit Ethernet line card (1X10GE-LR-SC) may crash, reporting %TX192-3-CPUIF errors.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 when you shut down the 10GE port of a 4-port 10 Gigabit Ethernet module (WS-X6704-10GE) that is installed in a Cisco 7609 at the other side of the connection.

  Workaround: There is no workaround.

- CSCee67207

  Symptoms: A public recursive route is not labeled.

  Conditions: This symptom is observed on a Cisco router that functions as a BGP peer and that has the **neighbor** *name* **send-label** command enabled as part of an IPv4 address family, which is required for Inter-AS configurations. The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

  Workaround: There is no workaround. Note that the symptom does not occur if the **neighbor** *name* **send-label** command is enabled as part of an IPv4 address family VRF.

- CSCee67746

  Symptoms: E4+ POS cards reporting %TX192-3-PAM_MODULE and %TX192-3-PAM_PIM errors. On rare occasions, the card may crash due to receiving malformed packet.

  Conditions: This symptom is observed with Cisco IOS Release 12.0(25)S3.

  Workaround: There is no workaround.

- CSCee68666

  Symptoms: It may take up to 1 second for a line card to notify the RP about a physical layer failure alarm. This situation prevents fast sub-second IGP convergence.

  Conditions: This symptom is observed in a non-FRR and non-APS configuration.

  Workaround: There is no workaround.

- CSCee69861

  Symptoms: When a host sends a path MTU discovery packet into a L2TPv3 tunnel, a Cisco 10720 returns an ICMP unreachable packet, indicating that the path MTU is “MTU-32byte (L2TPv3 header)-(layer2 header of customer packets),” which is incorrect. This situation causes TCP communications such as FTP or HTTP downloads over the L2TPv3 tunnel to fail. For example, 26 bytes (outer IP + L2TPv3 header sizes) may be missing.

  Conditions: This symptom is observed on a Cisco 10720 that functions as a PE router.

  Workaround: If this is an option, set an MTU with a small size at the server side. If this is not an option, there is no workaround.

- CSCee70024

  Symptoms: LSP-Ping packets may include a Vendor Enterprise Code TLV Type 5 with a length that is greater than 4 and with Vendor Private Extensions. According to the draft-ietf-mpls-lsp-ping-05.txt IETF draft, the Vendor Enterprise Code TLV Length should always be 4, and the vendor extensions should use a TLV Type that is in the range 64512-65535.

Conditions: This symptom is observed on a Cisco platform that functions in an MPLS OAM environment.

Workaround: There is no workaround.

- CSCee70478

  Symptoms: If hardware multicast forwarding is enabled on an Engine 2 line card that is connected to the source of multicast traffic, multicast traffic may not be forwarded after the router has reloaded.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(27)S2.

  Workaround: Remove and reapply hardware multicast forwarding to the line card.

- CSCee71793

  Symptoms: Malformed MPLS echo request packets may cause excessive Route Processor (RP) CPU cycles to be consumed during parsing of malformed TLVs.

  Conditions: This symptom is observed when MPLS echo request packet are decoded and incorrectly parse beyond the packet boundary due to improper bounds checking.

  Workaround: There is no workaround.

- CSCee72027

  Symptoms: WRED does not share WRED labels even when WRED parameters are identical. Because Engine 4 and Engine 4+ line cards have only seven WRED labels, when you configure WRED for all eight IP precedences, the line cards display the following error:

  ```
  % Can not configured WRED, all WRED labels are in use.
  ```

  This situation prevents part of the **precedence** (WRED group) command for the 8th IP precedence from being applied to the interface policy map.

  Conditions: This symptom is observed when you apply a policy map that uses more than seven WRED labels and when WRED labels are not shared.

  Workaround: There is no workaround.

- CSCee72353

  Symptoms: An LDP session over a tunnel interface may drop and not come back up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S when auto-tunnel traffic engineering is configured and when RSVP label distribution and LDP are configured in the MPLS core.

  If the **no mpls ip** command is configured on the physical interface to disable LDP, and RSVP label distribution remains enabled, auto-tunnel traffic engineering fails and you cannot bring the tunnel back up.

  Workaround: Run LDP in the MPLS core for all interfaces that have auto-tunnel traffic engineering configured.

- CSCee74886

  Symptoms: After you enter the **microcode reload pxf** command or after a PXF crash occurs, EoMPLS packets that should be encapsulated with EoMPLS encapsulation are treated as if they are normal IP packets, and are likely to be dropped by the router.

  Conditions: This symptom is observed on a Cisco 10720 router when an SRP (sub)interface is used as the EoMPLS backbone interface to transport EoMPLS packets to other EoMPLS PE routers and when the (sub)interface has the **xconnect** *destination-address vc-id* **encapsulation mpls** command enabled.

Workaround: Remove the **xconnect** *destination-address vc-id* **encapsulation mpls** command from the (sub)interface that connects to a customer device, and reconfigure it on the (sub)interface.

- CSCee75225

  Symptoms: High CPU utilization may cause interfaces to flap, and the following spurious memory access messages may be generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x603C2724 reading 0x194
  %ALIGN-3-TRACE: -Traceback= 603C2724 601D2888 601D40B4 00000000 00000000 00000000
  00000000 00000000
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(23)S when you the **clear cef linecard** command.

  Workaround: There is no workaround.

- CSCee76306

  Symptoms: A Cisco router crashes during a period of high routing protocol activity.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(21)SP or a later release or Release 12.0(22)S or a later release.

  The crash is most likely to occur when the router holds a large number of IPv4 prefixes in its routing table and when there is a lot of turnover in the routing table, that is, prefixes are added and deleted on a rapid basis.

  Workaround: There is no workaround.

- CSCee76476

  Symptoms: A Cisco 12000 series equipped with Engine 4 or Engine 6 line cards may crash because of an unexpected exception to CPU vector 300 when the CISCO-CLASS-BASED-QOS-MIB is queried via SNMP.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S or an earlier 12.0 S release.

  Workaround: There is no workaround other than excluding the access to the MIB.

- CSCee76995

  Symptoms: A packet becomes corrupted when you ping a POS line card.

  Conditions: This symptom is observed on a Cisco 12000 series Engine 0 4-port OC-3 POS line card. It only affects a Cisco IOS interim release of Release 12.0(29)S.

  Workaround: There is no workaround.

- CSCee77227

  Symptoms: When a channel group is removed and re-added to the controller, and then a PRE switchover occurs, the PPP line protocol on the re-added channel goes down after a while.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 24-port channelized E1/T1 line cards.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCee77328

  Symptoms: The PXF forwarding engine on a Cisco 10720 may crash after the microcode is reloaded either through a manual reload by entering the **microcode reload pxf** command or after a previous PXF crash. This situation causes multiple PXF crashes.

Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(26)S or a later Cisco IOS Release 12.0 S release, all of which contain IPv6 PXF packet forwarding functionality, and is most likely to occur while IPv6 packets are passing through the router.

Workaround: Disable IPv6 functionality or disable PXF by entering the **no service pxf** command.

- CSCee78118

  Symptoms: A line card or port adapter may crash on an MPLS VPN PE router when the customer-facing interfaces are flapped.

  Conditions: This symptom is observed when any of the following conditions are present:

  – eBGP is used as the routing protocol between the PE and CE router, the CE router has the **redistribute connected** command enabled in the BGP configuration, and there are multiple eBGP sessions between the PE and CE router.

  – The connected route for the link between the CE and PE router is learned from another PE router via MP-iBGP. For example, the CE router may be dual-homed and may advertise the connected routes to both PE routers.

  The symptom affects routers that perform MPLS forwarding using ASICs such as some Cisco 7200 series routers, the Cisco 7304, the Cisco 10000 series, the Cisco 12000 series, and the Cisco RPM-XF. (This list may not be exhaustive.)

  Workaround: Avoid the above-mentioned conditions. For example, avoid the **redistribute connected** command in the BGP configuration of the CE router.

- CSCee78567

  Symptoms: A temporary counter condition in which you see very large MPLS TE tunnel counter spikes may occur on a Cisco 12000 series. This situation is observed via the SNMP variable IfHCOutOctets (the total number of octets transmitted), via the SNMP variable locIfOutBitsSec (the Cisco 5-minute decaying average), and in the output of the **show interfaces tunnel** *number* privileged EXEC command (observe the elevated output rate).

  Conditions: This temporary counter condition is observed only for one or two sample periods and affects the MPLS-TE auto-bandwidth mechanism because the collection timer may be invoked at a time while the counter is at an extreme value. If the auto-bandwidth mechanism collection value is greater than the physical interface capability, the LSP tunnel build fails at the next LSP tunnel build.

  Workaround: There is no workaround.

- CSCee80041

  Symptoms: A line card with an ATM QoS configuration may crash.

  Conditions: This symptom is observed on a Cisco 12406 that runs a Cisco IOS interim release of Release 12.0(29)S. However, this caveat is resolved in Release 12.0(29)S.

  Workaround: There is no workaround.

- CSCee80214

  Symptoms: When you delete shaping by entering the **no shape** *cir* command, shaping seems to be disabled on all interfaces, which can be seen in the output of the **show policy-map interface** *interface-name* command. However, the output of the **show policy-map** *policy-map* command still shows the shape value.

  Conditions: This symptom is observed on Frame Relay subinterfaces on a Cisco 10000 series.

  Workaround: Remove and reconfigure the Frame Relay class on each subinterface or remove the policy map from the map class and reconfigure the policy map.

- CSCee82088

  Symptoms: The **show controller au-4** command does not show any detail tug groups under the controller.

  Conditions: The symptom was observed on the Cisco 10000 router with a channelized STM-1 linecard.

  Workaround: Issuing the following commands on the router will restore the au-4 controller display.

```
router# config terminal
router(config)# hw-module slot <slot number> shutdown
router(config)# no hw-module slot <slot number> shutdown
router(config)# end router#
```

- CSCee84193

  Symptoms: All interfaces in a multilink group go down when you enter the **no shutdown** command on the MLP interface.

  Conditions: This symptom is observed when the MLP interface is in the up/up state.

  Workaround: Do not enter the **no shutdown** command on an MLP interface that is already in the up/up state.

- CSCee84933

  Symptoms: A 1-port 10-Gigabit Ethernet line card (1X10GE-LR-SC) may crash, reporting a stack trace pointing to the optics interrupt handler.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 when you shut down the 10GE port of a 4-port 10 Gigabit Ethernet module (WS-X6704-10GE) that is installed in a Cisco 7609 at the other side of the connection.

  Workaround: There is no workaround.

- CSCee90155

  Symptoms: A TLU memory leak occurs on an Engine 3 line card that has aggregate IPv6 labels when the associated IPv6 route is flapped or changed.

  Conditions: This symptom is observed when you inject static routes that point out of a Gigabit Ethernet (GE) interface of a 4-port GE ISE line card and when the GE interface is flapped.

  Depending on the number of aggregate IPv6 labels, the TLU memory leak can be either service-impacting or very minor.

  Workaround: There is no workaround.

- CSCee90295

  Symptoms: A Cisco 12000 series may reload when configuring a large number of class-maps.

  Conditions: This symptom is observed on a Cisco 12816 router that has a PRP and that is running Cisco IOS Release 12.0(28)S.

  Workaround: Configure maximum 255 classes per parent policy-map.

- CSCee90552

  Symptoms: When you send an SNMP query to poll the CBQOS MIB, high CPU utilization may occur. Depending on number of service policies attached, the CPU utilization may reach 100 percent, causing many different negative effects to occur: the Telnet connection may go down, LDP may go down, and in some cases the router may crash.

  Conditions: This symptom most likely occurs when the unsupported cbQosREDClassStats objects are polled and when there are about 1000 QoS policy attachment configured.

Workaround: The potential workarounds include the following:

- Reduce the number of QoS policy attachments.
- Avoid polling the unsupported stats table(s).
- Reduce the polling frequency.

- CSCee90590

  Symptoms: A 6-port OC-3 POS line card (ESR-6OC-3/P-SMI=) may go down unexpectedly, and the following error messages may be logged (assuming that the line card is installed in slot 6 of the router):

  ```
  IPCOIR-4-REPEATMSG: IPC handle already exists for 6/0
  IPCOIR-2-CARD_UP_DOWN: Card in slot 6/0 is down. Notifying 6oc3pos-1 driver.
  C10K_ALARM-6-INFO: ASSERT CRITICAL slot 6 Card Stopped Responding OIR Alarm -
  subslot 0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(27)S2 in a dual-PRE configuration when the CPU utilization on the active PRE is high. The symptom may also occur in other 12.0 S releases.

  Workaround: There is no workaround.

- CSCee90893

  Symptoms: An RP may crash if a policy map matches a QoS group value that is greater than seven.

  Conditions: This symptom is observed on an interface of a Cisco 12000 series Engine 4+ line card when the interface is configured for shaping.

  Workaround: Use a QoS group value in the range of one through seven in the policy map.

- CSCee93228

  Symptoms: Under certain unknown circumstances, a traceroute may trigger a process watchdog.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2. However, the problem is not specific to a Cisco 12000 series or to Cisco IOS Release 12.0S and may occur on other platforms and in Release 12.2T and Release 12.3.

  Workaround; There is no workaround.

- CSCef01537

  Symptoms: A VIP may reload because of a bus error when a corrupted FIBIDB is used unchecked by the router.

  Conditions: This symptom is observed rarely on a Cisco 7500 series when MQC is configured.

  Workaround: Disable the MQC configuration.

- CSCef01689

  Symptoms: Transient errors may be generated when you boot a 1-port channelized OC-48/STM-16 (DS3/E3, OC-3c/STM-1c, OC-12c/STM-4c) POS/SDH ISE line card. The errors disappear after some time.

  Conditions: This symptom is observed on a Cisco 12000 series when you boot the card line card by reloading either the router or the line card itself. The symptom occurs only when the peer router sends RIPv1 packets.

  Workaround: There is no workaround.

- CSCef03176

  Symptoms: A ping between two GRE interfaces may not work.

Conditions: This symptom is observed when a GRE tunnel between two routers is up and you ping from the GRE interface of one router to the GRE interface of the other router.

Workaround: There is no workaround.

- CSCef08774

  Symptoms: Certain types of fragmented packets are dropped when the ingress line card is an E6 line card and the egress line card is an E4+ line card. (CSCed22100 addresses this symptom for the E4+ line card.)

  Conditions: This symptom is observed on a Cisco 12000 series when there is an Engine 1 GE line card along the path before the traffic enters the E6 line card and when this Engine 1 GE line card does not have any features enabled.

  Workaround: Configure a feature such as Sampled NetFlow on the Engine 1 GE line card.

- CSCef09884

  Symptoms: The RP that is supposed to become the primary RP may crash when an RP switchover occurs.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Cisco IOS Release 12.0(26)S3. This caveat is resolved in Release 12.0(26)S3.

  Workaround: There is no workaround.

- CSCef11214

  Symptoms: An Engine 2 Quad OC-12 POS line card release may fail when it is processing traffic.

  Conditions: This symptom is observed on a Cisco 12000 series that runs a Cisco IOS interim release of Release 12.0(26)S3. This caveat is resolved in Cisco IOS Release 12.0(26)S3.

  Workaround: There is no workaround.

- CSCef12828

  Symptoms: When traffic passes through a router, the router blocks traffic for certain prefixes behind a port-channel link. Traffic that originates from the router itself (that is, process-switched traffic) works fine.

  Conditions: This symptom is observed on a Cisco 12410 that runs Cisco IOS Release 12.0(27)S1 and that is configured with two PRP-2 processors.

  Workaround: There is no workaround.

- CSCef13024

  Symptoms: An Engine 2 line card in a Cisco 12000 series router does not forward packets destined to default route in hardware. Instead it is routed through the line card CPU.

  Conditions: Cisco IOS Release 12.0(27)S2 is affected by this problem.

  Workaround: There is no workaround. Traffic goes through the local CPU and so performance might be an issue.

  Further Problem Description: This problem is a side effect of the caveat CSCdz42137.

- CSCef14150

  Symptoms: The **show policy-map interface** command and its corresponding MIB, CISCO-CBQOS-MIB, report no or fewer Random Drops than what the router actually drops.

  Conditions: The problem occurs only on interfaces at or faster than 500 Mbps.

  Workaround: There is no workaround.

- CSCef16326

  Symptoms: When you remove a policy map from a subinterface, the subinterface may become stuck, preventing traffic from passing through the subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0(25)SX7 when a nested policy map is applied to the main or physical interface in addition to the one that is already applied to the subinterface. The symptom could also occur in Release 12.0S.

  Workaround: Remove the policy map from the physical interface before you remove the policy map from the subinterface. When the subinterface configuration is updated, re-apply the policy map to the physical interface.

- CSCef23821

  Symptoms: Packet latency in a priority class is high when shaping is enabled in the parent class. For example, when you send 400 kbps of traffic through the priority class, the measured latency is about 80 ms.

  Conditions: This symptom is observed when the service policy has a shape average of 768000 on the class default and a child policy with a priority feature.

  Workaround: There is no workaround.

- CSCef24642

  Symptoms: The PXF engine on a Cisco 10720 may crash, and the following error messages are generated in the logging buffer (the PXF crashinfo files can be found in the flash memory of the router):

  ```
  MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T0 IHB Exception: watchdog
  MSD: %TOASTER-2-FAULT: T1 IHB Exception: watchdog
  ```

  In addition, there are four ways to verify that the symptom is occurring:

  – If the **debug main error**, **debug uplink error**, and **debug access error** commands are enabled on the router, the following error messages are also generated in logging buffer:

    ```
    MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error SRP_TX_VA_SC_GIANT_PKT
    (code 4)
    MSD: %Camr_SRP_OC48-3-INTERR: SRP uplink internal error
    SRP_TX_VA_SC_FIFO_GIANT_PKT(code 100)
    MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error
    VA_SC_IPM_RD_ACC_TIMER_EXP(code 1)
    MSD: %Camr_VA-3-STATUS1: Van Allen Data integrity error
    VA_RP_IPM_RD_ACC_TIMER_EXP(code 4)
    MSD: %Camr_VA-3-SISTATUS: Van Allen SRIC Data integrity error
    VA_SI_FL_CTRL_DRVN(code 80)
    MSD: %Camr_VA-3-SOSTATUS: Van Allen SROC Data integrity error VA_SO_PKT_LEN_ERR
    (code 1)
    MSD: %Camr_VA-3-STATISTICS: VA statistics register: 0x0098 reports
    VA_SO_PKT_LEN_ERR_COUNT =  3
    ```

  – In the output of the **show interface srp 1/1** command, the received error counters such as “framer runts” and “input errors” have a large value.

  – In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the “destination unreachable” counter increases.

- In the output of the **show hard pxf cpu statistics interface srp 1/1 detail** command, the "zero encap length" counter increases.

Conditions: This symptom is observed when all of the following conditions are present:

- A packet enters with or without an MPLS label.
- The router tries to send an ICMP packet to the source in any of the following situations:
  * The packet is denied by an output security ACL.
  * There is no route in the router to forward the packet.
  * The time to live (TTL) of the packet expires.
  * The packet is an ICMP echo request packet, and the router tries to send an ICMP echo reply packet to the source.
- On the interface on which the packet enters, the **ip unreachable** command is enabled by default.

Workaround: Enter the **no ip unreachable** command on all interfaces of the router, which works in the following two cases:

- The packet is denied by an output security ACL.
- There is no route in the router to forward the packet.

For other cases, there is no workaround.

- CSCef25866

  Symptoms: Connectivity for destinations that are reachable via an MPLS TE tunnel may fail when the tunnel is fast-rerouted. The loss of connectivity may result in loss of TCP sessions (BGP, LDP, etc.) for those destinations.

  When the problem happens, the output of the **show ip cef** *network* command shows "invalid cached adjacency" for the tunnel but does not show "fast tag rewrite."

  Conditions: This symptom is observed when all of the following conditions are present:

  - The adjacency of the primary tunnel becomes incomplete when FRR is active, as can be observed in the output of the **show adjacency** *type number* command. Whether or not the adjacency becomes incomplete is media-dependent. For example, with PPP the adjacency becomes incomplete but not with HDLC.
  - The primary tunnel is the only path to reach the prefix in question.
  - The **ip cef accounting non-recursive** command is not enabled.
  - A routing change occurs for the prefix after the FRR switchover. (This is topology dependent)

  Workaround:

  - Use HDLC encapsulation instead of PPP. This will prevent the adjacency from becoming incomplete.
  - Use forwarding adjacencies. This will prevent the routing change.

  Further Problem Description: The symptom affects traffic that originates on the tunnel headend. Transit traffic going through the tunnel is not affected. The symptom does not occur if there are multiple paths to the destination (one of which is the tunnel).

- CSCef25872

  Symptoms: An OC192E/POS-IR-SC line card in a Cisco 12000 series may crash with the following messages:

  ```
  %GRP-4-RSTSLOT: Resetting the card in the slot: 4,Event: linecard error report
  %MDX-1-DAEMSGSNDFAILED: FAILED to send IPC message of TYPE MDX_DAE_PULL_REQ to
  slot 4 on the DAE,
  ```

```
        FAIL REASON = retry queue flush
%LCINFO-3-CRASH: Line card in slot 4 crashed
```

Conditions: The symptom is seen when the ciscoOpticalMonitoringMIB is polled on a router running Cisco IOS Release 12.0(27)S1. The card that crashes does not have to be the card that is being polled. For example, an OC192E/POS-VSR in slot 0 may be polled with 1.3.6.1.4.1.9.10.83.1.1.1.1.8.2 and the OC192E/POS-IR-SC in slot 4 may crash.

Workaround: Stop the crashes by configuring an SNMP view that prevents the ciscoOpticalMonitoringMIB from being polled.

- CSCef29224

  Symptoms: When removing or modifying a service-policy from a MFR or MLPPP bundle CFI, there is an RP crash.

  Conditions: This symptom is observed on a Cisco router in which a police-policy is applied on the bundle CFI over an ISE 1xOC12 Channelized to DS1 Line Card.

  Workaround: There is no workaround.

- CSCef31934

  Symptoms: In a scaled configuration with hundreds of eBGP peers with very low BGP timers, issuing **clear ip bgp *** may increase HW forwarding memory utilization.

  Conditions: This problem is seen with 500 eBGP sessions with BGP keepalive timer of 3 seconds and hold timer of 9 seconds. The router has 200K MPLS VPN routes. This problem is not seen if the BGP timers are set to the default value.

  Workaround: There is no workaround.

- CSCef37186

  Symptoms: The Simple Network Management Protocol (SNMP) agent may use 99 percent of the CPU bandwidth of a Route Processor (RP) for an arbitrarily long time, possibly generating CPUHOG errors and causing a watchdog crash. Other processes on the router may fail because these processes do not receive the CPU bandwidth that they require. Consequently, the following difficulties may occur:

  - Routes may time out.
  - Tunnels may go down.
  - Accessing the router via a Telnet connection to a network port may become impossible.
  - The command-line interface (CLI) via the console line may become quite slow to respond.

  The output of the **show snmp summary** EXEC command may indicate that the number of requests is “N” while the number of replies that were sent is “N-1.” The output of the **show processes cpu | include SN** EXEC command may indicate that the SNMP process uses 99 percent of the CPU bandwidth of the RP.

  Conditions: These symptoms are observed on a Cisco 7300 series when the MPLS-LSR-MIB MIB is enabled, when you query the object mplsXCIndexNext, and when there are more than 1,000 Multiprotocol Label Switching (MPLS) labels active. However, the symptoms are platform-independent.

  Workaround: Perform the following steps:

  1. Shut down interfaces to bring the total count of active MPLS labels down to far below 1,000.
  2. Disable the MPLS-LSR-MIB MIB by entering the following sequence of commands:

     ```
     snmp-server view nolsrmib mplsLsrMIB exclude
     snmp-server view nolsrmib iso include
     ```

3. Modify each defined community string to include the **view nolsrmib** keywords. For example, define the "public" community string by entering the following command:

   ```
   snmp-server community public view nolsrmib ro
   ```

4. Enter the **no shutdown** interface configuration command on all the interfaces that you shut down in Step 1.

- CSCef37716

  Symptoms: An LSP ping may not interoperate with third-party vendor equipment. The following commands may either timeout or receive an error return code from third-party vendor equipment:

  – **ping mpls ipv4** *ip-address address-mask*

  – **trace mpls ipv4** *ip-address address-mask*

  – **ping mpls pseudowire** *peer-id vc-id*

  Conditions: This symptom occurs because of recent changes to the ietf-mpls-lsp-ping-06.txt draft, preventing Cisco's implementations of LSP pings from interoperating with third-party vendor equipment.

  The recent draft changes include the following:

  – "Implicit padding" of the Target FEC TLV subtype lengths is required when pinging an LDP IPV4 FEC.

  – The FEC definition that is used in the **ping mpls pseudowrire** command now requires Target FEC TLV subtype 10 instead of 9.

  Workaround: There is no workaround.

- CSCef39381

  Symptoms: When 1000 input ACLs are configured on an Engine 3 line card and when traffic is denied by the input ACL, the following error message and traceback are displayed continuously on the console:

  ```
  %GRP-4-NO_INTF: CSAR: No interface available Slot 4 Chan 19
  -Traceback= 1ADD94 44A2E4 44A988 44BD94 44C3D0 4451D8 27CCB0
  ```

  This symptom occurs whether the router is configured with a GRP, a PRP-1, or a PRP-2. When the router is configured with a PRP-1 or PRP-2, the output of the **show controllers psar | incl idb** shows the following:

  ```
  No IDB drops - 3423 IDB queue tail drops - 0 CORE2-R2#
  ```

  However, the output of the **show idb** command shows that there are 32 IDBs.

  When the router is configured with a GRP, the output of the **show controllers csar** does not show anything unusual.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2a only when an input ACL is applied, when traffic is denied by the input ACL, and when the **ip unreachable** command is enabled on the interface of the Engine 3 line card.

  Workaround: Enter the **no ip unreachable** command on the interface of the Engine 3 line card.

- CSCef40187

  Symptoms: An SRP interface is stuck and there is no response at all. In the output of the **show srp topology** command, the last topology packet that is received takes more than five seconds to arrive. In addition, the "zero encap length" counter in the output of the **show hardware pxf cpu stat interface srp 1/1 detail** command increases.

  Conditions: This symptom is observed on a Cisco 10720 when the value of the overall packet size divided by 32 is 1 or 2.

Workaround: There is no workaround.

- CSCef41460

  Symptoms: GRE tunnel may not work on a PE router if VPN is configured.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(25)S or a later release.

  Workaround: There is no workaround

- CSCef42706

  Symptoms: CPUHOG conditions, BGP sessions flaps, and APS channels flaps are observed on a router.

  Conditions: These symptoms are observed when SNMP is polled on a Cisco 12000 series that has about 500 interfaces and subinterfaces and more than 900 attached service policies. The router may produce CPUHOG log messages when the CISCO-CLASS-BASED-QOS-MIB stats are polled.

  Workaround: There is no workaround.

- CSCef42815

  Symptoms: A flap of the BGP session between a primary provider edge (PE) router and a customer edge (CE) router that provides the default route may cause a remote CE router to lose Internet connectivity when the BGP session is restored.

  Conditions: This symptom is observed in a topology with CE routers that are dual-homed and connected to two Cisco 12000 series routers that function as PE routers and that run Cisco IOS Release 12.0(26)S2 when the default route is generated by a CE router in a different VPN routing/forwarding (VRF).

  Workaround: There are two steps to the workaround:

  1. Add a default VRF static route to cover the BGP-derived default route.
  2. Clear the default route entry in the routing table.

- CSCef42849

  Symptoms: Timing violation occurs in the PRE2/PRE1 temperature sensor routine. Since the temperature sensor routines violate timing requirements, the temperature reading fails in new device from a new vendor.

  Conditions: The failure occurs only in new temperature sensor from new vendor. All old type of sensors are not effected.

  Workaround: There is no workaround.

- CSCef44154

  Symptoms: When an MPLS packet that enters through an SRP or Ethernet interface contains an L2TP or UTI packet and this MPLS packet is processed by the RP instead of the PXF engine (for example, when the IP header in the MPLS packet contain options and the MPLS TTL equals 0 or 1), the SRP or Ethernet interface stops receiving packets.

  Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0S.

  Workaround: There is no workaround.

- CSCef44274

  Symptoms: The per-WRED-class drop counters are not incremented under “show queueing” output even though the aggregate WRED drops are non-zero.

  Conditions: Problem is specific to legacy random-detect command enabled under the main interface.

Workaround: Attach a policy-map to the interface with random-detect enabled.

- CSCef45609

  Symptoms: An Engine 3, QOC12 LC configured with Multicast VPNs, may punt traffic to RP if multicast is disabled using the **no ip multicast-routing distributed** command and then re-enabled using the **no ip multicast-routing distributed** command.

  Conditions: This symptom is observed on a Cisco 12000 series that is running the gsr-p-mz image of any Cisco IOS Release from 12.0(26)S4.

  Workaround: There is no workaround.

- CSCef48325

  Symptoms: WRED counters do not function on distributed platforms such as a Cisco 7500 series and a Cisco 7600 series.

  Conditions: This symptom is observed on a a distributed Cisco platform that runs Cisco IOS Release 12.0(26)S3, 12.0(29)S, 12.2(25)S, 12.3(10), or 12.3(11)T and that has dWRED configured.

  Workaround: There is no workaround.

- CSCef48573

  Symptoms: An Engine 3 Quad OC-12 line card that is configured with multicast VPNs may punt traffic to the Route Processor (RP).

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of a Cisco IOS interim release for Release 12.0(30)S. Note, however, that this caveat is resolved in Release 12.0(30)S.

  Workaround: There is no workaround.

- CSCef49138

  Symptoms: The **sh policy-map int a7/3.201** command causes the router to crash by bus error exception.

  Conditions: The router crashes when the configuring the **service-policy out lanqos** command on the interface ATM7/3.201 and issuing the **sh policy-map int a7/3.201** command.

  Workaround: There is no workaround.

- CSCef52419

  Symptoms: In Cisco IOS software versions prior to Cisco IOS Release 12.0(27)S3, Release 12.0(28)S1, and Release 12.0(30)S, the Cisco 10720 router CPU utilization is high (x%/y%), where y is greater than 60%, and is reporting continuous BGP and LDP flapping. The **show interface** counters are showing a large number of drops and the **show buffers** command shows a large number of cache misses for the private IBC buffer pools.

  Conditions: The Cisco 10720 router is in a broadcast ARP storm environment and the interface **holdq <queue length> in** queue length is not the default of 75 packets for any one of the router's interfaces (for example, it is 2048).

  Workaround: Revert the **holdq <queue length> in** and **holdq <queue length> out** to the default setting by using the **default holdq in** and **default holdq out** commands on all interfaces with non-default hold queues.

- CSCef54021

  Symptoms: The sync message configures the same queue number for both policies on the secondary RP. The code now after the fix handle each policy separately syncing the right queue number for each policy.

Conditions: This symptom occurs after an SSO switch over traffic stopped for interfaces having both input and output policy attached.

Workaround: Remove and reattach the policy to the interface.

- CSCin24544

  Symptoms: A permanent virtual connection (PVC) configuration is removed if a PVC fails when it is recreated.

  Conditions: This symptom is observed on a Cisco 7500 series that has a Versatile Interface Processor (VIP). The PVC configuration may be removed if the VIP is carrying data traffic and the parameters of the virtual circuit (VC) class that is attached to the configured PVCs on the associated interface are modified.

  Workaround: There is no workaround.

- CSCuk51177

  Symptoms: You may not be able to make a Telnet connection to a Cisco IOS platform.

  Conditions: This symptom is observed when the CNS Exec Agent is used to remotely issue an interactive CLI command.

  Workaround: There is no workaround.

- CSCuk51269

  Symptoms: Multicast packets such as HSRP and OSPF are not received on a port-channel interface.

  Conditions: This symptom is observed when a port-channel interface is configured on a Cisco router, when you reload the router, and when the first member is added to the port-channel interface by entering the **no shutdown** interface configuration command on physical interface.

  Workaround: Enter the do **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port-channel interface.

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages.
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
  3. Attacks that use ICMP “source quench” messages.

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Wide-Area Networking

- CSCdx84284

  Symptoms: A router may not recognize some inbound Multiprotocol Label Switching (MPLS)-tagged packets that are sent via Frame Relay. Because the router cannot recognize the inbound MPLS-tagged packets, MPLS cannot switch those packets to the outgoing interface. The MPLS-tagged packets are dropped by the router, and the router does not increment the input-packet counter in the output of the **show frame pvc** output EXEC command.

  Conditions: This symptom is observed on a Cisco router that has Cisco Express Forwarding (CEF) enabled and that is running Cisco IOS Release 12.2(7b). The symptom may also occur in other releases.

  Workaround: Enable the **debug mpls packets** EXEC command.

- CSCed02028

  Symptoms: A router may reload unexpectedly because of a bus error after the following error message is displayed:

  ```
  %ATMPA-3-BADVCD:ATM[int] bad vcd [number] packet -
  ```

  Conditions: This symptom is observed on a Cisco router that is configured with an ATM interface when a packet that contains a virtual circuit descriptor (VCD) that is out range is passed on to the ATM driver of the interface in order to be transmitted.

  Workaround: There is no workaround.

- CSCee15586

  Symptoms: A Cisco 7500 series may crash when you configure a T1 channel group.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or 12.0(27)S when the same channel group was previously configured for Frame Relay encapsulation, when one or more PVCs on the channel group were configured on the main interface with a map class that contained a service policy, when the channel group was deleted, and when the map class definition that it referenced was also deleted.

  Workaround: Remove the Frame Relay encapsulation before you delete the channel group.

Resolved Caveats—Cisco IOS Release 12.0(27)S2

Cisco IOS Release 12.0(27)S2 is a rebuild of Cisco IOS Release 12.0(27)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(27)S2 but may be open in previous Cisco IOS releases. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCed32794

  Symptoms: Executing the **tftp-server slaveslot0:** global configuration command, or any configuration commands related to tftp-server being set to access flash devices on the slave, will cause the slave to reload.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0(23)S5 but is not platform dependent.

  Workaround: Configure the tftp-server to access flash devices on the master route switch processor (RSP) only.

- CSCed47820

  Symptoms: The Remote Processing Time reported by an SAA probe to a VRF/VPN loopback on a MPLS VPN PE router is too short, about 1~30ms, while the Round Trip Time that is calculated is too large, about >100ms. When you have probes sent to both an IPv4 Loopback and a VPNv4/VRF Loopback, you will see that the results they provide are exactly reverse to each other. For example:

  ```
  router time type remote process time roundtrip delay saa_probe2ipv4 218 1
  saa_probe2vpnv4 5 219
  ```

  Conditions: This symptom is observed when an SAA probe is sent to VPN/VRF addresses on an MPLS VPN PE router through a MPLS VPN network.

  Workaround: There is no workaround.

- CSCee55603

  Symptoms: SNMP request to VRF interface on PE router should be restricted with SNMP ACL following the **snmp-server community** command, but it does not work.

  ```
  snmp-server community community-name [ro | rw] access-list-number
  access-list access-list-number {permit | deny} address mask
  ```

  Conditions: This symptom is observed in Cisco IOS Release 12.0(27)S or later releases and is platform independent.

  Workaround:

  – Use an SNMP Context-Based ACL, which can choose each VRF.

    ```
    snmp-server community community-name [ro | rw]
    snmp mib community-map community-name target-list vpn-list-name
    snmp mib target list vpn-list-name {vrf vrf-name | host ip-address}
    ```

  – Use the **snmp-server drop vrf-traffic** command if you want to discard any SNMP request through VRF.

- CSCin67568

  Symptoms: A Cisco device experiences a memory leak in the CDP process.

  Conditions: The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.

Interfaces and Bridging

- CSCec87736

  Symptoms: TX Simple Network Management Protocol (SNMP) counters do not update on Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic.

  Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S and Release 12.3. The hardware is DEC21140A, and the interface receiving the traffic is not located on the same Versatile Interface Processor (VIP).

  Workaround: There is no workaround.

- CSCed08399

  Symptoms: A Cisco 7500 series may generate spurious memory accesses at a VIP.

  Conditions: This symptom is observed when CRTP is enabled on the interfaces of the VIP.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCec07636

  Symptoms: When the following Open Shortest Path First (OSPF) MIB tables are queried via snmpwalk, some interfaces may not be displayed:

  - ospfNbrTable

  - ospfIfTable

  - ospfIfMetricTable

  Conditions: This symptom is observed on any Cisco platform that runs OSPF.

  Workaround: There is no workaround.

- CSCed00449

  Symptoms: SAA probes that are executing on the Cisco 12000 series routers incorrectly measure round trip time delay measurements.

  Conditions: This symptom is only observed on a Cisco 12000 series router.

  Workaround: Run the probe on a different Cisco platform.

- CSCed62901

  Symptoms: This symptom occurs in an OSPF network topology in which a CE router (CE-1) connect to a PE router (PE-1) that connects to two other PE routers (PE- 2 and PE-3), each of which connect to another CE router (CE-2 and CE-3). In turn, both of these CE routers are connected to each other (that is, CE-2 and CE-3 connect to each other).

  When the link between the PE-3 and the CE-3 flaps, the OSPF route in the VRF fails to switch back from BGP to OSPF on the PE-1.

  Conditions: This symptom is observed in Cisco IOS Release 12.0 S, 12.2 S, and 12.3 T.

  Workaround: Clear the ip route, clear the OSPF process, or enter the **clear ip bgp *** command on the PE-1 to bring the route back from BGP to OSPF.

- CSCed70979

  Symptoms: A router may reload unexpectedly with a bus error and/or display spurious memory access messages.

  Conditions: This symptom is observed when the router is configured for OSPF and is actively learning OSPF routes dynamically.

  Workaround: There is no workaround.

- CSCed75295

  Symptoms: FRR LSPs may fail to provide protection with a Next-next-hop (NNHOP) backup tunnel.

  Conditions: This symptom is observed only when a primary LSP reaches beyond a merge point.

  Workaround: There is no workaround.

- CSCed82273

  Symptoms: IPv6 BGP may not reach the established state.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0(26)S2 or Release 12.0(28)S. However, the symptom is not platform-specific.

  Workaround: There is no workaround.

- CSCee10426

  Symptoms: A BGP prefix may receive or advertise incorrect label information.

  Conditions: This symptom is observed on an MPeBGP session between ASBRs when there is more than one MPeBGP session configured.

  Workaround: There is no workaround.

- CSCee36622

  Symptoms: ABRs may continue to generate summary LSA(s) for obsolete non-backbone intra-area route(s).

  Conditions: This symptom occurs under the following conditions:

  1. The ABR (call ABR X) has at least one non-backbone area (call area X) in common with one or more additional ABRs.
  2. The ABRs are generating summary LSAs, on behalf of the Area X's two or more intra-area routes, into the backbone area and other areas. The two intra-area routes must be advertised as stub links from two different routers; i.e., one from ABR X, and the other from another router belonging to Area X.
  3. The summary LSA IDs for the intra-area routes above, when ORed with the host bits of the corresponding masks, yield identical LSA IDs.

     For example, 10.10.10.128/25 and 10.10.10.0/24 yield identical LSA IDs when the network address is logically ORed with the host bits; i.e.,

     ```
     10.10.10.128 | 0.0.0.127 = 10.10.10.255
     10.10.10.0   | 0.0.0.255 = 10.10.10.255
     ```

  Workaround: Perform the **clear ip ospf proc** command on all ABRs containing the obsolete LSAs.

- CSCee42285

  Symptoms: Non-EIGRP originated routes are not supported. Furthermore, when a route is injected into mp-BGP from a connected, static, or any other IGP on the remote PE router where the same prefix is also learned via EIGRP (when a backdoor exists for that site), the route may constantly flap between EIGRP and BGP.

  Conditions: These symptoms are observed when the EIGRP MPLS VPN PE-CE SoO feature is configured.

  Workaround: Only inject EIGRP routes into mp-BGP for sites with a backdoor.

ISO CLNS

- CSCed40888

  Symptoms: A Border Gateway Protocol (BGP) session may be terminated unexpectedly.

  Conditions: This symptom is observed on a Cisco router that functions as a peer in a BGP configuration when you disable and reenter the **neighbor** *ip-address* **send-label** address family configuration or router configuration command or when you move the router that has the **neighbor** *ip-address* **send-label** address family configuration or router configuration command enabled to a peer group.

  Workaround: There is no workaround.

- CSCee54672

  Symptoms: The redistribution of routes from L1 into L2 or/and from L2 into L1 may not occur properly, and a learned IS-IS prefix may be missing.

  Conditions: This symptom is observed under the following conditions:

  – There are multiple paths to reach the same prefixes.

  – One source LSP removes a prefix and another LSP adds the same prefix, while both paths between the prefix and the LSPs are of equal cost.

  Workaround: Enter the **clear isis *** or the **clear ip route *** command to restore the prefix. However, doing so clears all the routes and recalculates them again, which is a disruptive action.

Miscellaneous

- CSCdy40928

  Symptoms: Connectivity difficulties may occur when Virtual Private Network (VPN) routing/forwarding (VRF) packets follow the global routing table instead of the VRF table.

  Conditions: This symptom is observed on a low-end Cisco router that runs Cisco IOS Release 12.2(7a) or another release when the global address space in the router overlaps with the VRF address that is configured on a VRF interface of a connected PE router. The VRF interface of this PE router may be unreachable but end-to-end connectivity may not be affected.

  Workaround: There is no workaround.

- CSCea28043

  Symptoms: IP commands that are sent in the Cisco Networking Services (CNS) config-changed event output may contain an extra **ip** prefix.

Conditions: This symptom is observed on a Cisco router when you enter both **ip** global configuration commands and the **cns config notify** *diff* global configuration command to capture commands that change configuration for the config-changed event output.

Workaround: Enter the *all* keyword in the **cns config notify** global configuration command. This workaround is not valid when the only changes in the configuration occur in the config-changed event output.

- CSCeb52330

  This caveat consists of two symptoms, two conditions, and two workarounds.

  1. Symptom 1: The interface commands in the CNS configuration notify changed message contain unexpected data.

     Condition 1: This symptom is observed when you configure the CNS **cns config notify** *diff* global configuration command and you configure **interface** global configuration commands on the Cisco IOS device.

     Workaround 1: There is no workaround if only the changes in the configuration are expected in the CNS configuration notify changed message.

     Alternate Workaround 1: Specify the *all* option for the cns config notify global configuration command.

  2. Symptom 2: Once the **cns config notify** global configuration command is configured, the router may not detect a newly created interface.

     Condition 2: This symptom is observed when the *diff* option in the **cns config notify** global configuration command is selected and a new dynamic interface is created.

     Workaround 2: There is no workaround.

- CSCeb73894

  Symptoms: You may not be able to load a Cisco IOS software image onto a Cisco 12000 series from an Advanced Technology Attachment (ATA) Flash disk, and one or more error messages similar to the following may appear:

  ```
  open(): Open Error = -13 loadprog: error - on file open boot: cannot load
  "disk0:gsr-p-mz.120-24.S2"
  ```

  ```
  open: read error...requested 0x4 bytes, got 0xffffffff trouble reading device magic
  number loadprog: error - on file open boot: cannot load "disk0:gsr-p- mz.120-22.S3c"
  ```

  Conditions: This symptom is observed when the ATA disk is formatted with one Cisco IOS software image and also contains another Cisco IOS software image that you attempt to load onto the Cisco 12000 series.

  Workaround: Enter the **boot system tftp** *filename ip-address* global configuration command, **dummy** for the *filename* argument, and **10.1.1.1** for the *ip-address* argument. Note that this command parses without errors, and then fails; the router may not appear to boot initially, but eventually does so.

  Further Problem Description: The symptom only affects a Cisco 12000 series RP. It does not affect a Cisco 12000 series PRP.

- CSCec45307

  Symptoms: There may be no memory for the expanded TFIB PSA. The label allocation may fail with error messages that are shown below and may be followed by a memory traceback.

  ```
  %TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag
  ```

  ```
  %TFIB-2-MEMORY: No memory for expanded TFIB PSA
  ```

  ```
  -Traceback=
  ```

Conditions: This symptom is only observed on an MPLS-capable Cisco platform and only when the label space has been exhausted to the maximum level supported by the platform or is about to be exhausted (only a few hundred labels are available) and when the TFIB table is expanded further.

Workaround: Enter the **mpls label range 16 101900** command at the conf-t level to avoid the error messages.

- CSCec46191

  Symptoms: When you securely copy a Cisco IOS image to a flash disk by entering the **copy scp slot0:** or **copy scp slot1:** EXEC command, the copy process may stop after about 60 to 70 percent has been transferred.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(25)S1 or Release 12.3.

  Workaround: Copy the Cisco IOS image via another transport protocols such as TFTP.

- CSCec77049

  Symptoms: The adjacency table is not retained after an RP switchover.

  Conditions: This symptom occurs with a 4-port Ethernet PA inside a VIP4-80 on an RSP 16.

  Workaround: Clear the adjacency table with the **clear adjacency** command after the Stateful Switchover (SSO).

- CSCec78545

  Symptoms: A Versatile Interface Processor (VIP) may reload when the **clear cef line** command is entered or when a new VRF is provisioned on an interface via the CLI.

  Conditions: This symptom is observed on a VIP when Multiprotocol Label Switching (MPLS), Egress NetFlow, and distributed Cisco Express Forwarding (dCEF) are configured.

  Workaround: Disable dCEF or Egress NetFlow before making configuration changes or before entering the **clear cef line** command.

- CSCec80283

  Symptoms: An IP Services Engine (ISE) line card may display high CPU utilization.

  Conditions: This symptom is observed on an ISE line card in a Cisco 12000 series when Multiprotocol Label Switching (MPLS) packets are sent to the nonlabel-switched interface of the ISE line card.

  Workaround: There is no workaround.

- CSCed08168

  Symptoms: No SNMP linkup or linkdown trap is generated for a 1CHOC12/4CHSTM1 SONET layer when a controller goes up and down.

  Conditions: This symptom is observed when monitoring a SNMP linkup or linkdown trap for a 1CHOC12/4CHSTM1 SONET layer.

  Workaround: Monitor the controller status using the **show controller sonet** command.

- CSCed10965

  Symptoms: All line cards may crash due to an IPC timeout or fabric ping timeout.

  Conditions: This symptom is observed on a Cisco 12000 series with a PRP under heavy traffic conditions. The output of the **show controllers psar** command shows excessive error events (e.g. free queue empty events).

Workaround: There is no workaround. The fix for this DDTS adds the new **show monitor event-trace psar** command to show any bursty error events that are traced but not visible in the output of the **show logging** command.

- CSCed15913

  Symptoms: An Engine 0 12xE3 line card may reload when changing the MTU on an Engine 2 3x1GE line card.

  Conditions: This symptom is observed on a Cisco 12416 router that is running the gsr-p-mz image of Cisco IOS Release 12.0(26)S.

  Workaround: Ensure there is no traffic going through the Engine 0 12xE3 and Engine 2 3x1Ge line cards when attempting to change the MTU.

- CSCed21111

  Symptoms: There is no console response from the primary or secondary route processor.

  Conditions: This symptom occurs after the **redundancy force-failover main-cpu** EXEC command is sent for the second cutover.

  Workaround: There is no workaround.

- CSCed22358

  Symptoms: A Cisco 12000 series may forward packets to an incorrect interface. This behavior can been seen by looking at the hardware CEF entry on this input line card:

  ```
  execute-on slot x show ip hardware-cef a.b.c.d (a.b.c.d is the destination IP address)
  ```

  The output looks similar to the following, in which the CEF lookup is null:

  ```
  LC-Slot0#show ip hardware-cef a.b.c.d Leaf FCR 2 0x784C6FC0 found 2 deep alpha ip
  loadbalance: 0x78198D00 - lbl not equal. cef lookup NULL
  ```

  After clearing the route, the output looks as follows:

  ```
  LC-Slot0#show ip hardware-cef a.b.c.d Leaf FCR 4 0x784C6FC0 found 2 deep Fast
  Adjacency: alpha adjacency: 0x701E8280 [0-7] oi 0x4019100 oq 4000 in 15 ab 0 hl 20 gp
  11 tl 0 loq BC01 15/0 mtu 4470 packets 1750013440 bytes 776867999767

  Output Queue / Local Output Queue Bundle: [0-7] output queue 0x4000 local output queue
  0xBC01
  ```

  This problem may cause packets to be dropped because a loop is created and the TTL expires for the packets.

  Conditions: This symptom is observed under very specific conditions on a Cisco 12000 series that runs Cisco IOS Release 12.0(24)S or a later release when traffic that enters an Engine 3 line card toggles between a static-to-null route and a more specific route as the destination.

  Workaround: Avoid the specific conditions mentioned above. Clearing the route resolves the problem only temporarily.

- CSCed28604

  Symptoms: Enabling autonegotiation on an E1 Gigabit Ethernet interface causes the standby route processor (RP) to fail.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(26)S.

  Workaround: Stop the traffic, enter the **shutdown** command on the interface, configure autonegotiation on the interface, enter the **no shutdown** command on the interface, and resume the traffic.

- CSCed30253

  Symptoms: WRED classification may fail.

  Conditions: This symptom is observed when you configure WRED and pass traffic.

  Workaround: There is no workaround.

- CSCed32758

  Symptoms: A reload or online insertion and removal (OIR) of any line card on a Cisco 12000 series Internet router chassis with a 1+1 Automatic Protection Switching (APS) configuration between two CHOC-48 line cards may cause a "deadman timer expired" error. This may result in an incorrect switch working once the line card comes up.

  Conditions: This symptom is observed on a Cisco router with a channelized OC48 line card that is running the c12kprp-p-mz image of Cisco IOS Release 12.0(24)S4.

  Workaround: There is no workaround.

- CSCed37615

  Symptoms: A router may reload unexpectedly after renaming a policy-map the second time.

  Conditions: This defect may be observed if there are at least two policies configured.

  Workaround: Avoid renaming the policy-map.

- CSCed41067

  Symptoms: When the cache is lost, a router correctly detects that the cache is no longer available, but HTTP requests are still forwarded to the cache.

  Conditions: This symptom is observed on a Cisco 7500 series with dCEF enabled.

  Workaround: Disable dCEF.

- CSCed44319

  Symptoms: A file that is copied to an ATA disk may become corrupted.

  Conditions: This symptom is observed on any Cisco IOS image that contains the fix for CSCdz27200. The problem does not occur on a disk that is formatted with 16 or less sectors/cluster.

  Workaround: Use an ATA disk that is formatted with 16 or less sectors/cluster. The **show disk all** command indicates how many sectors are configured per cluster.

- CSCed45460

  Symptoms: The **hw-module slot** *slot-number* **ip multicast hw-accelerate source-table size 4096 offset 0** command is not synced to a standby RP if a line card is reloaded while the standby RP is booting.

  Conditions: Symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

  Workaround: Wait until the standby RP is fully operational before entering the above-mentioned command.

- CSCed45746

  Symptoms: Several prefixes for non-redistributed connected interfaces in different VRFs may be partially bound to the same MPLS-VPN label, thus disrupting traffic bound to one or more of these VRFs.

  Conditions: This symptom can occur on a Cisco router that runs Cisco IOS Releases 12.2, 12.2T, 12.0S, 12.3 after the VRF interfaces have flapped. The symptom may occur in all code levels of these releases.

  Workaround: Clear the routes in the VRFs in sequence.

- CSCed46184

  Symptoms: VPN sessions may not be established.

  Conditions: This symptom is observed in an Xconnect configuration when a CFI interface goes down after the VPN service is being established. This is a timing issue.

  Workaround: Remove and reconfigure Xconnect.

- CSCed46669

  Symptoms: On a Cisco 12000 series in a dual-RP (GRPs or PRPs) SSO mode, when certain configuration commands are typed such as a nested **policy-map** command, the standby RP may crash. While the RP reboots after the crash, it is not available to perform its standby function.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(22)S or a later release. A nested **policy-map** command can cause this problem. In general, any configuration command that uses a large amount of processor stack space, such as the nested **policy-map** command may, may cause the standby RP to crash.

  Workaround: There is no workaround.

- CSCed46747

  Symptoms: After an SSO and before a standby RP is completely up, when you perform and OIR of line cards, a configuration synchronization failure may occur and the standby RP may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S when you perform an OIR of an 8-port Packet-over-SONET OC-3c/STM-1 single mode line card and a 4-port ISE Packet-over-SONET OC-12c/STM-4 single mode/IR SC connector line card.

  Workaround: Perform an OIR of these line cards after the standby RP is up.

- CSCed48941

  Symptoms: A Cisco MGX 8800 series Route Processor Module XF (RPM-XF) may crash and generate the following error message:

  No memory for XCM tempbuffer logged

  Conditions: This symptom is observed on an RPM-XF that functions as a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when you enter the **clear interface sw1** command multiple times on the RPM-XF.

  Workaround: There is no workaround. The fix for this caveat is also integrated in images that support the Cisco 10000 series, such as Cisco IOS Release 12.0 S.

- CSCed49303

  Symptoms: A Cisco 12000 series that runs 12.0(25)S2 may report the following log message:

  ```
  SLOT 1: %SYS-3-CPUHOG: Task ran for 2052 msec (1/1), process = CEF LC IPC Background,
  PC = 400DC728.

  -Traceback= 400DC730 40DBFE60 40DBFFD4 40DC0B14 400C5A04 400C59F0
  ```

  Conditions: This symptom is observed when the default route gets updated to Engine 3 line cards and is reported by these line cards as seen above. This situation may happen after an interface flap or a routing update elsewhere in the network.

  To determine if your line card is an Engine 3 line card, enter the **show diag** *slot-number* EXEC command, in which the *slot-number* argument is the slot number that reports the message). In the command output, you will see "L3 Engine: 3" for Engine 3 line cards.

  Workaround: There is no workaround.

- CSCed51371

  Symptoms: Intermittent packet drops occur when you ping the VRF loopback/interfaces on a PE router from an attached PE router. The VPN transit traffic intermittent drops occur also on packets that exceed the MTU size.

  Conditions: This symptom is observed on a Cisco 12000 series 3-port GE and 4-port GE line card that are installed in a Cisco router that functions as a PE router and that is connected to another PE router via an L2 switch. The problem occurs when a VRF is configured on a subinterface that faces the L2 switch.

  Workaround: Remove the VRF from the subinterface that faces the L2 switch.

- CSCed52163

  Symptoms: When the HSRP MIB is polled and there are HSRP groups configured on subinterfaces, an error such as "OID not increasing" may occur on the device that is polling the router. In some cases, a CPUHOG traceback may occur on a router when the HSRP MIB is polled, especially when a lot of interfaces are configured.

  Conditions: This symptom is observed under either one of the following two conditions:

  - An SNMP HSRP query triggers a loop in the getnexts. Some MIB browsers catch this, and exit with a message stating "OID not increasing."

  - A scaling problem may occur with HSRP when there are a high number of tracked interfaces. For every standby track statement, every interface is tested to see if it is an HSRP tracked interface. No defined thresholds have been identified and tested that qualify when this scaling problem may occur. The more interfaces there are configured, the greater is the possibility that the problem occurs.

  Workaround: Do not initiate an SNMP query for HSRP.

  Alternate Workaround: Enter the **snmp-server** global configuration command to specify which MIBs are available, as in the following example:

  snmp-server view *HSRP* **internet included**

  snmp-server view *HSRP ciscoHsrpMIB* **excluded**

  snmp-server view *HSRP ciscoHsrpExtMIB* **excluded**

  snmp-server community public view *HSRP RW 20*

  snmp-server community private view *HSRP RW 20*

- CSCed52578

  Symptoms: The MPLS packets are forwarded with a bogus label when they are sent out on a loadshared non-VRF MPLS enabled "Internet" interface from a VRF.

  Conditions: A static route for the VRF should be configured to reach the Internet, which would in turn be configured to recourse over 2 static routes to reach the next hop for the global Internet.

  Workaround: Shut down one of the interfaces to remove the load-sharing condition.

- CSCed54080

  Symptoms: Per VPN per destination load balancing is not operating correctly on an Engine 2 or 4+ that is running Cisco IOS Release 12.0(23)S4 and seems to be load sharing only on BGP nexthop.

  Conditions: There are no specific conditions.

  Workaround: The **clear ip route vrf** *vrf- name* command invokes a recalculation on the hashes. Also, the **clear ip bgp** *neighbor* **soft** command (can) reassign(s) new labels and respread(s) the load. These commands may impact service by stopping traffic forwarding.

- CSCed54262

  Symptoms: Memory allocation (MALLOC) failures may occur on a VIP, port adapter, or line card.

  Conditions: This symptom is observed on a Cisco router that has a scaled AToM configuration.

  Workaround: There is no workaround.

- CSCed56025

  Symptoms: A VIP, port adapter, or line card may reset.

  Conditions: This symptom is observed on a router that has a scaled AToM configuration.

  Workaround: There is no workaround.

- CSCed56092

  Symptoms: A standby GRP or PRP may keep resetting.

  Conditions: This symptom is observed on a Cisco 12000 series when you change releases from Cisco IOS Release 12.0(27)S to another release using the **hw-module standby reload** command and when the RPR mode is enabled.

  Workaround: Enter the **reload** command.

- CSCed56404

  Symptoms: On a Cisco 12000 series with link-bundling (port-channel) configured and the **snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart** command configured, if you configure the port-channel with minimum links that are greater that the actual links, the port-channel is forced down, and an SNMP linkdown trap is generated. However, if you correct the configuration so that the port-channel comes up, no linkup trap is generated.

  Conditions: This symptom is observed on a Cisco 12000 series router that runs Cisco IOS Release 12.0(26)S1.

  Workaround: There is no workaround.

- CSCed57281

  Symptoms: A router may log a CPUHOG message that is caused by the CEF reloader process.

  Conditions: This symptom is observed on a Cisco router when a VRF with more than 9000 routes is added to the configuration.

  Workaround: There is no workaround.

- CSCed57625

  Symptoms: An access control list (ACL) that has logging enabled may not work on a Fast Etherchannel (FEC) interface.

  Conditions: This symptom is observed on a Cisco 10720 router running Cisco IOS Release 12.0(26)S or a later release.

  Workaround: There is no workaround.

- CSCed57841

  Symptoms: When the error message “Info: Illegal normal burst size, increased to mtu size 4470” is generated on a channelized STM-1 MM PA, the VIP in which this PA is installed and the RSP may crash.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S1 when MQC is configured on the channelized STM-1 MM PA.

  Workaround: There is no workaround.

- CSCed57925

  Symptoms: The **cisco.mgmt.cns.config-changed** event message does not get generated when **atm pvc** CLIs are configured.

  Conditions: This may occur when the CNS configuration notify agent is configured by the **cns config notify** configuration command and **atm pvc** CLIs are configured.

  Workaround: There is no workaround.

- CSCed59020

  Symptoms: An Engine 1 single port Gigabit Ethernet line card for a Cisco 12000 series router may reload unexpectedly on receipt of large amounts of "pause input" frames sent via flow control from a downstream device.

  Conditions: This symptom will occur only if the Gigabit Ethernet line card is forwarding large amounts of traffic to an overwhelmed downstream device that in turn sends "PAUSE" (XOFF) frames to the line card.

  Workaround: Disable flow control on the downstream device.

- CSCed59500

  Symptoms: During SB HA test, there is continuous traceback which shows there is an unrecognized CPU q.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed60987

  Symptoms: On a Cisco 7500 series with distributed CEF, connectivity between CE routers that are locally connected to the same interface may be broken.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or a later release when an output service policy is configured on the subinterface of one CE router but not on the subinterface of the other CE router. Traffic that is process-switched flows correctly between the CEs routers.

  Workaround: Configure a dummy output service policy on the subinterface that does not have an output service policy.

- CSCed61577

  Symptoms: After executing a forced switchover, the secondary processor returns only to COLD standby and not HOT standby.

  Conditions: This symptom is observed on a c10k-p10-mz image on a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCed63480

  Symptoms: The **hw-module** {**slot** *X*} command shutdown on a 4GE Eng3 that is using GEC may freeze a router during some time, bringing down line and protocols. Under certain circumstances, DCEF may also be disabled.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed64461

  Symptoms: Frame Relay local switching fails when RED is applied on a Cisco 12000 series router with a 2-port OC-3 channelized to DS1/E1 line card or a 6- port channelized T3 line card.

Also, it is observed that the controller is reset when the following is removed/reapplied:

```
rx-cos-slot all ToFabTable
!
  slot-table-cos ToFabTable
  destination-slot 0 OC3
  destination-slot 1 GIGE
```

Conditions: This symptom is observed on a Cisco 12000 series router.

Workaround: Perform the following steps:

1. Remove the RED configuration.
2. Reload microcode onto the line card (a 2-port OC-3 channelized to DS1/E1 line card or a 6-port channelized T3 line card).
3. Reapply the RED configuration.

- CSCed65027

  Symptoms: When the MTU is toggled from 4470 to 9180 or 64, a 4xOC12 ATM line card may enter the "ERR CARV" state and does not recover. Even reloading the line card does not bring it back up.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the gsr-p-mz image of Cisco IOS Release 12.0 S.

  Workaround: Reload the router.

- CSCed66001

  Symptoms: A %LINK-4-TOOBIG error message may appear on the console log of a Cisco 10000 series.

  Conditions: This symptom is observed when you send a ping or an L2TP packet across an MPLS interface that is configured for label imposition.

  Workaround: There is no workaround.

- CSCed66160

  Symptoms: A Cisco router crashes while verifying if FRR is active at Backup Head.

  Conditions: A show display of a large number of FRR Active LSPs (Label Switched Paths) issued by the **show mpls traff fast database int xx** command was paused before completing when one of the LSPs was deleted by an external event. When the display was resumed, the deallocated LSP was referenced by the show display causing the router to crash.

  Workaround: There is no workaround.

- CSCed66388

  Symptoms: A 4-port OC-12 ISE ATM card may crash when an L3 PVC is configured on a main interface, a service policy is attached to the L3 PVC, and there are F4 OAM VCs on the same the main interface. F4-OAM VCs are created when there are VP tunnels or layer 2 VPs that perform cell relay/cell packing.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed69722

  Symptoms: When a recursively resolved adjacency is "discard" (e.g., null0), a packet that is entering an Engine 3 4-port GE line card and that is destined to the "discard" adjacency is punted to the local line card CPU, causing high CPU utilization. Punting to the CPU is caused by a wrong adjacency that is populated for the corresponding route.

Conditions: This symptom is observed on Engine 3 line cards that are installed in a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S1 or a later release.

Workaround: There is no workaround.

- CSCed70822

  Symptoms: With four fabric cards (one CSC in slot 16 and three SFCs), after a power cycle, the line cards fail to come up and fabric ping timeouts occur.

  Conditions: This symptom is observed on a Cisco 12000 series and affects all E4 and E4+ cards.

  Workaround: Place a CSC card in slot 17. The fix for this caveat applies to all types of line cards (E0, E2, E3, E4 and E4+).

- CSCed71467

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: When a policy map is applied under an L2VPN (AToM: CRoMPLS) ATM PVC on a Cisco 12000 series Engine 3 ATM card, it is not possible to get class-map or policy-map statistics. When you enter the **show policy map interface** command, the following message is seen:

  ```
  Class statistics not available.
  ```

  This message is seen on a policy map without policing, and in this specific case, the policy map uses a class-default match and sets the MPLS EXP bits.

  Condition 1: This problem is seen when a policy map that does not include any policing is applied to a Cisco 12000 series Engine 3 ATM line card that is configured for AToM/L2VPN.

  Workaround 1: Enable policing to get the policy-map and class-map statistics.

  Symptom 2: If a policy map that involves policing is applied L2VPN (AToM: CRoMPLS) ATM PVC on a Cisco 12000 series Engine 3 ATM card, the policy-map statistics are available but the following incorrect message shows up at the top of the output of the **show policy map interface** command:

  ```
  NOTE: Statistics are aggregated for all the VC's in the subinterface
  ```

  This statement is not true because the per VC policy-map statistics are available in the case of L2VPN PVCs on this line card.

  Condition 2: This problem is seen when the same policy map as in Condition 1 is modified to include policing.

  Workaround 2: There is no workaround.

- CSCed72340

  Symptoms: Some MQC commands on 4xOC3 and 8xOC3 ISE line cards on Cisco 12000 series routers may result in a message similar to the following:

  ```
  % Service policy on FR sub-interface POS1/1.2 must be hierarchical.
  ```

  Due to the error, no policy is applied to the interface. Even though the running configuration has the policy on the interface, the policy will not take effect.

  Conditions: This symptom is observed on Cisco 12000 series routers.

  Workaround: There is no workaround.

- CSCed72686

  Symptoms: An ACL applied to an ATM subinterface (RFC1483) may not work after a PRE switchover.

  Conditions: This problem is observed on a Cisco 10008 router with PRE2.

  Workaround: Deconfigure and configure again the access list that is not working.

- CSCed73722

  Symptoms: On an Engine 3 4GE line card, traffic from a Catalyst switch to a Cisco 12000 series is not rerouted over the GEC link when disabling the physical interface on which the traffic is passing.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S1.

  Workaround: There is no workaround.

- CSCed73780

  Symptoms: An EPA-GE/FE-BBRD line card may experience repetitive crashes during normal operation.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S2 or 12.0(26)S1.

  Workaround: There is no workaround.

- CSCed74617

  Symptoms: After an RPR+ switchover, the output information of a tag adjacency is replaced by the output information of the corresponding IP adjacency. This situation causes MPLS traffic forwarding to stop.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as a PE router and that is configured with AToM VCs after a switchover in RPR+ mode has occurred.

  Workaround: There is no workaround.

- CSCed74917

  Symptoms: An ACL applied to a subinterface may becomes active on the main interface, without showing this in the configuration.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(25)S2.

  Workaround: Do not apply the ACL to the subinterface.

- CSCed75108

  Symptoms: When an IP VRF is configured on an SDCC interface of a Cisco 10720 router, all MPLS packets which are to be forwarded through the SDCC interface are instead dropped by the PXF forwarding engine.

  Conditions: This problem is observed when setting up an MPLS-VPN in which the PE-CE interface is an SDCC interface on the Cisco 10720 router.

  Workaround: Disable the PXF forwarding path via the **no service pxf** command.

  Further Problem Description: The forwarding path must deal with MPLS packets that are destined for the SDCC interface by punting them rather than dropping them.

- CSCed75233

  Symptoms: A line card crashes when the CPK internal debug tool is enabled because of uninitialized data in the CPK debug code.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed75347

  Symptoms: CR and CPK VP policing is broken when a mux-ed PVC VCI range is above 4095.

Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S.

Workaround: There is no workaround.

- CSCed77178

  Symptoms: HSRP configured on the subinterfaces of an Engine 4+ GE line card may not work.

  Conditions: This symptom is observed when the subinterfaces are configured with VRFs.

  Workaround: There is no workaround.

- CSCed78519

  Symptoms: SCR continues to filter CLP(0) cells and tag CLP(1) cells when the CLP(0) filter is removed from the **class-map** command.

  Conditions: This symptom is observed when there are multiple PVCs and when the class map filters are globally removed.

  Workaround: There is no workaround.

- CSCed78847

  Symptoms: Cisco Express Forwarding (CEF) becomes disabled on a secondary Cisco 10000 series Performance Routing Engine (PRE) during a switchover.

  Symptoms: This symptom is observed after configuring 380 traffic engineering (TE) tunnels and checking that CEF is enabled on both the primary and secondary PREs and that all TE tunnel interfaces are up. Then, a forced switchover from the primary PRE to the secondary PRE is performed. When the secondary PRE comes up and it now the new primary PRE, all tunnel interfaces are down. The line is up but the protocol is down. Because CEF is disabled and not running, the tunnels do not function and no routing can occur.

  Workaround: Enable CEF on the primary PRE and enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces. Doing so enables the TE tunnels to come up.

- CSCed79804

  Symptoms: A CRoMPLS pseudowire may fail to come up.

  Conditions: This symptom is observed on a Cisco 12000 series when the disposition is changed from an Engine 4+ line card to an Engine 2 ATM OC-12 line card.

  Workaround: There is no workaround.

- CSCed81349

  Symptoms: A standby RP may fail when MPLS TE tunnels are configured.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S.

  Workaround: There is no workaround.

- CSCed81644

  Symptoms: Using Cisco IOS Release 12.0(28)S images on Cisco 12000 series routers and Engine-6 2xOC192 line cards, the **show interface accounting** command shows incorrect values for tag packets.

  Conditions: This symptom is observed during a tag->tag scenario.

  Workaround: Ignore the IP counters for the tag packets.

- CSCed82152

  Symptoms: An Engine 4+ line card may reset and generate errors.

Conditions: This symptom is observed after a manual RP switchover in RPR mode.

Workaround: There is no workaround.

- CSCed83256

  Symptoms: A Cisco 12000 series may hang when you enter the **no shutdown** or **atm ilmi-pvc** command.

  Conditions: This symptom is observed on a Cisco 12406 that runs the grp-p-mz image of Cisco IOS Release 12.0(28)S and that is configured with dual GRPs and a 4-port OC-12 ATM ISE line card.

  Workaround: There is no workaround.

- CSCed83434

  Symptoms: On a line card, the VPN prefixes in one VRF may be attached to another VRF.

  Conditions: This symptom is observed when more than one VRF is configured in nonalphabetical order and a when an RPR+ switchover occurs.

  Workaround: After configuring VRFs, reload the router before a switchover can occur.

- CSCed84331

  Symptoms: MPLS TE tunnel counters are inaccurate; the MPLS TE tunnel output rate counters may exceed the physical interface capabilities that the tunnel uses.

  Conditions: This symptom is seen on a Cisco 12000 series that runs Cisco IOS Release 12.0(23)S5 with an Engine 4 line card. This symptom may be observed by issuing the following commands in the following order:

  1. Enter the **show interfaces tunnel** *number* command. This command tells you the interface statistics for the tunnel.
  2. Enter the **show mpls traffic-eng tunnels** *tunnel-interface* command. This command tells you the physical interface the tunnel traverses.
  3. Enter the **show interfaces** *type slot/port* command. This command tells you the physical interface statistics.

  Workaround: There is no workaround.

- CSCed84474

  Symptoms: After an APS switch using channelized OC-12 line cards (channelized to DS-1), some Frame Relay interfaces may fail to carry traffic.

  Conditions: This symptom is observed on a Cisco 12000 series with an OC-12 line card (channelized to DS-1) with a linear APS configuration.

  Workaround: If an individual interface does not recover on its own, enter the **shutdown** command followed by the **no shutdown** command on the affected interface.

- CSCed85073

  Symptoms: For MVPN traffic, multicast traffic streams are punted from the PXF to the RP. Normally, PXF does this when a new stream needs to be created. However in this case, PXF behaves as if the streams are not present even if the required (S,G)/(*,G) states exist.

  Conditions: This symptom is observed on a Cisco 10000 series when the VRF index of the VPN is higher than 255. This occurs when 255 or more VRFs are configured or when some VRFs are created and deleted many times. You can determine the VRF index by entering the **show ip vrf detail** command.

  Workaround: There is no workaround.

- CSCed85570

  Symptoms: When a POS card is shut down, the show facility status still indicates alarms. When a line card is shut, there should be no alarms for that card.

  Conditions: This symptom is observed on Cisco 10000 series.a POS line card.

  Workaround: There is no workaround; ignore the alarms in the show facility status, it is a display error.

- CSCed86596

  Symptoms: IPv4 multicast traffic may stop being forwarded when NetFlow is configured on an Engine 4+ interface.

  Conditions: This symptom is observed on a Cisco 12000 series that runs the Cisco IOS Release 12.0 S when a (*,G) entry is used to forward IPv4 multicast traffic instead of a (S,G) entry.

  Workaround: There is no workaround.

- CSCed86694

  Symptoms: When APS is configured, traffic stops flowing after you perform an OIR on two line cards (each line card once).

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround. To reenable the traffic flow, reset both line cards at the same time (that is, one immediately following the other).

- CSCed86984

  Symptoms: CEF may become disabled on a VIP, port adapter, module, or line card because of a fatal error, and the following error message may be generated:

  %FIB-3-FIBDISABLE: Fatal error, slot 2: Window did not open, LC to RP IPC is non-operational

  Conditions: This symptom is observed after an RPR+ switchover.

  Workaround: There is no workaround.

- CSCed88967

  Symptoms: When you enter the **write memory** command, two files may be missing (“persistent-data” and “rf_cold_starts”) or the following error message may be displayed:

  ```
  startup-config file open failed (Device or resource busy)
  ```

  Conditions: This symptom is observed on any router with redundant RPs running any Cisco IOS release when the following sequence occurs:

  - You enter the **write memory** command on the console of the master RP.
  - The NVRAM of the standby RP is accessed by a local application (that is, the application on the standby RP).
  - A switchover occurs.

  Workaround: Do not access the NVRAM of the standby RP when you enter **write memory** command on the console of the master RP.

- CSCed89518

  Symptoms: MPLS IAS traffic may be punted the CPU of an Engine 2 line card.

  Conditions: This symptom is observed when an egress interface is flapped and the ingress POS-channeling interface is shut down in a topology in which the ingress POS-channeling interface connects to an ASBR that connect to the egress POS interface.

  Workaround: There is no workaround.

- CSCed89629

  Symptoms: A VIP4-80 may crash when you enter the **police** command for a policy map that is applied to an ATM subinterface PVC in the input direction.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(26)S or 12.0(27)S.

  Workaround: Do not enter the **police** command for a policy map that is applied to an ATM subinterface PVC.

- CSCed89963

  Symptoms: A Cisco 12000 series may experience a block overrun and redzone corruption with a subsequent system reload or switchover as a result of incorrectly processing a corrupted packet. Error messages similar to the following may be observed:

  ```
  %GRP-4-CORRUPT: Corrupted packet, start_offset 96, length 65534, slot 9
  %SYS-3-OVERRUN: Block overrun at 53E4389C (red zone 00000000)
  ```

  Conditions: This symptom may be observed on a Cisco 12000 series that runs Cisco IOS Release 12.0 S and that has 1, 3, or 4 port Gigabit Ethernet line cards installed.

  Workaround: There is no workaround.

- CSCed90701

  Symptoms: The packet queue size on an MLP bundle may be larger than necessary, which may manifest as two separate symptoms:

  – The scalability during configuration of multiple MLPPP interfaces is reduced because the router may run out of resources to allocate the packet queues.

  – The effect of congestion may be more severe as traffic that should have been dropped due to the queue overflow will not be dropped.

  Conditions: This happens after the reload of a Cisco 10000 series with a policy map attached to an MLP interface or when more links are added to an MLP interface.

  Workaround: After any MLP bundle change (either by configuration, bootup, or link failure) delete and reattach the service policy to the interface.

- CSCed90731

  Symptoms: The priority traffic on an MLP interface may exceed the configured bandwidth limits.

  Conditions: This symptom is observed on a Cisco 10000 series when new links are added to an MLP interface that already has a policy map with a priority class attached. The link addition may happen as result of a system bootup or a link flap, or a user may add more links to the bundle by configuration.

  Workaround: Once the interfaces that are associated with the MLP bundle are up, remove and reattach the service policy to the MLP bundle. If links associated with the bundle flap, the policy may have to be removed and reattached again.

- CSCed90846

  Symptoms: A class that contains the **priority percent** *percent* command and that is loaded at or greater than the specified rate leaves other classes with less than their fair bandwidth and adversely affects their bandwidth ratio.

  Conditions: This symptom is observed on Cisco 10000 series network interfaces at or above OC-3 speed.

  Workaround: There is no workaround.

- CSCed91338

  Symptoms: An ATM device that is connected to a Cisco 12000 series may cause a communication failure because of a length mismatch between the ATM adaption layer 5 (AAL5) and the IP data length.

  Conditions: This symptom is observed when an IP frame that is smaller than 46 bytes in length comes from an Ethernet interface to an interface of an ATM line card (4OC3/ATM-IR-SC) on a Cisco 12000 series. The router always sets the length in the AAL5 to 54 bytes, as if the IP length is 46 bytes (which is the minimum length of the IP data plus an AAL5 header of 8 bytes).

  Workaround: There is no workaround.

- CSCed91389

  Symptoms: OAMs are dropped on a Cisco router's ATM IMA interface that is configured for AAL5oMPLs, causing directly connected CE routers that have the **oam pvc-manage** command enabled to take the PVC down. As a result, the CE routers cannot forward any traffic to the MPLS core, thereby impacting basic connectivity between CE routers that are interconnected via the MPLS core. Errors are also see when the **debug atm error** command is enabled.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.0(28)S and that is configured for AAL5oMPLS on an ATM-IMA interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCed92733

  Symptoms: On a Cisco 10720 router, when the system limit for the number of interfaces is surpassed, a software traceback is generated, indicating that a VCCI was not allocated. This traceback does not identify which interface caused the resource failure.

  Conditions: The problem is seen when the system limit on interfaces is reached. The most common scenario on a Cisco 10720 router is when the maximum number of VLANs is surpassed.

  Workaround: There is no workaround.

  Further Problem Description: The interface for which a VCCI is not allocated is not functional in PXF. The fix for this problem identifies that a resource allocation has failed and identifies which interface is affected.

- CSCed93139

  Symptoms: Local and remote attachment circuit "Up events" may be ignored.

  Conditions: This symptom is observed after a pseudowire virtual circuit is established.

  Workaround: There is no workaround.

- CSCed93593

  Symptoms: The **cisco.mgmt.cns.config-changed** event message contains invalid <changeItem> information.

```
Example: for:  (config)#policy-map TEST2
               (config-pmap)#class m_new
               (config-pmap-c)#shape peak 8010
               (config-pmap-c)#priority
               (config-pmap-c)#exit
               (config-pmap)#desc TESTTEST
               (config-pmap)#exit
The 4th changeItem is: Context:    <empty>
```

```
EnteredCmd: exit
NewConfig#: <empty>
OldConfig#:
            !
            MyPolicy
            test
            TEST2
            description TESTTEST
            class m_new
            shape peak 8010
            priority
```

Conditions: This may occur when the CNS configuration notify agent is configured by the **cns config notify** configuration command and policy-map CLI is configured on the Cisco IOS device.

Workaround: There is no workaround.

- CSCed94042

  Symptoms: A transient error may occur on a Cisco 12000 series line card during a network routing change. here is a chance that other line cards in the system will stop transmitting or receiving routing protocol updates and traffic, causing traffic to be blackholed.

  Conditions: This symptom is observed in an MPLS-VPN network. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb58214. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Enter the **microcode reload** command on any line card that stops receiving traffic or routing protocol adjacencies from its neighbors.

- CSCee00516

  Symptoms: An echo reply source address may be set incorrectly as 0.0.0.0 when responding to an echo request received on an unnumbered interface. Some line cards may check for the 0.0.0.0 source address condition and discard the packet based on that condition.

  Conditions: This symptom is observed during an LSP ping/traceroute. The symptom is platform independent.

  Workaround: Avoid using numbered interfaces. If this is not an option, there is no workaround.

- CSCee01931

  Symptoms: A router may crash when you enter the **fair-queue** command on the interface of a PA-MC-STM-1 port adapter.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S when the interface has the **rate-limit output** command enabled.

  Workaround: There is no workaround.

- CSCee02510

  Symptoms: High CPU utilization may occur on a Cisco 12000 series line cards due to the CEF scanner process.

  Conditions: This problem is seen when a large number of VPN routes are present on the router.

  Workaround: There is no workaround. However, the symptom does not seem to affect the convergence time or performance of the router.

- CSCee04454

  Symptoms: A Cisco 10000 series router reloads unexpectedly as ATM VCs are coming up.

  Conditions: This symptom is believed to occur only when ACLs are applied on ATM interfaces, and, only rarely then, on images that contain the CSCed72686 fix.

  Workaround: There is no workaround.

- CSCee05882

  Symptoms: The queue size may not be set up correctly after a Cisco 10000

  Conditions: This symptom is observed when an MLP bundle has an output policy attached to an interface and the service policy contains WRED parameters.

  Workaround: Remove and reattach the service policy to the MLP bundle interface after the router has reloaded.

- CSCee07446

  Symptoms: The **ping mpls pseudowire** and the **trace mpls pseudowire** commands may fail on a Cisco 12000 series.

  Conditions: This symptom is observed when you enter these commands for an Engine 3 line card.

  Workaround: There is no workaround.

- CSCee12772

  Symptoms: On certain platforms (in particular but not limited to a Cisco 800 series), the CNS agents code that captures output for later transmission can crash.

  Conditions: This symptom is observed on a router that has configuration and EXEC agents and CNS agents that execute CLI commands when you send an XML file to direct these agents to execute a CLI command and return the output (if there is any output).

  Workaround: Telnet into the router (not through the console) and exit. This may need to be done multiple times.

- CSCee16581

  Symptoms: Traffic is sent using the “net ctrl” queue on the egress interface.

  Conditions: This problem occurs on a Cisco 10720 router when IPv6 high-priority traffic (110 or 111 in the first 3 bits of the IPv6 traffic class) is forwarded.

  Workaround: There is no workaround.

- CSCee18844

  Symptoms: Traffic forwarding problems may occur when sending MVPN traffic from multiple sources to the same group.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as an MVPN decapsulation PE router with an Engine 3 line card that forwards multicast packets on an VRF interface.

  Workaround: To ensure that no collisions occur on the VRF interface, configure hardware multicast on the Engine 3 line card by entering the **hw-module slot** *number* **ip multicast hw-accelerate source-table size** *x* **offset** *y* command.

- CSCee19222

  Symptoms: An MLP bundle configured between a Cisco 7500 series and any other router may not be able to switch traffic when dCEF is enabled on the Cisco 7500 series.

Conditions: This symptom is observed when LFI is enabled with one member link in the MLP bundle.

Workaround: Either remove dCEF or remove LFI. (A combination of CEF and MLP is not supported.) Note that if there are two member links in the interleaving-enabled MLP bundle, the problem does not occur.

- CSCee22933

  Symptoms: CBR-type or VBR-type VP cell-relay or cell-packing AToM VCs may not be able to retain their bandwidth to the configured CBR or VBR shaping rate. This situation persists even when the total shaping rate of the VPs and VCs is far below the physical bandwidth of the interface.

  Conditions: This symptom is observed when there are many other cell-relay or cell-packing AToM VCs configured.

  Workaround: There is no workaround.

- CSCee24263

  Symptoms: A PVC may be inactive and may not come up.

  Conditions: This symptom is observed when a VC is deleted or removed and you try to recreate the same VC.

  Workaround: Save the configuration and reload the router.

- CSCee24389

  Symptoms: MPLS packets that are larger than 1496 bytes and that have the DF bit set are dropped, even when the **tag-switching mtu 1508** command is enabled on all interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series that is configured as an MPLS PE router, when all of the following conditions are met:

  - MPLS VPN packets enter through a 4-port Gigabit Ethernet (GE) ISE line card and leave from an ATM OC-3 Engine 0 line card
  - Output CAR is configured on the ATM interface.
  - You reload the router, reload the ATM line card, or enter the **shutdown** command followed by the **no shutdown** command on the ATM interface.

  Workaround: There are two workarounds:

  - Disable output CAR on the ATM interface and reboot the router.
  - Disable output CAR on the ATM interface and change the MTU or tag-switching MTU for the ATM subinterface.

- CSCee28754

  Symptoms: GE interfaces on an EPA-GE/FE-BBRD line card may drop tag packets.

  Conditions: The problem is reported on a Cisco 12000 series running Cisco IOS Release 12.0(23)S5 only when you perform an OIR of an EPA-GE/FE-BBRD to install or remove additional EPA-3GE-SX/LH line cards.

  Workaround: Perform a second OIR of the line card.

- CSCee29196

  Symptoms: When a Cisco 10000 series does not have a specific route for both end points of a voice connection, the Cisco 10000 series duplicates one-way audio only for the specific route that populates its routing table, not for the end point that uses the default route from the routing table.

  Conditions: This symptom is observed on a Cisco 10000 series that is runs Cisco IOS Release 12.0(25)S3 and that is configured with a PRE-1.

Workaround: There is no workaround.

- CSCee30089

  Symptoms: If a multilink interface loses members of the bundle, or if you enter the **shutdown** command followed by the **no shutdown** command on a multilink interface, or if the router reloads, the bandwidth that is allocated for non-real time classes can be allocated incorrectly. The sum of the bandwidth that is allocated for non-real time classes and the bandwidth that is specified by the **police** *bps* command for real time traffic may exceed the actual bandwidth of a multilink interface.

  Conditions: This symptom is observed on a Cisco 10000 series running Cisco IOS Release 12.0(27)S1 that has the **service-policy out** command enabled on a multilink interface. The service policy consists of a real-time class and several classes with reserved bandwidth The real-time class is configured with the **priority** command and the **police** *bps* command. Other classes are configured with the **bandwidth** *bandwidth-kbps* command.

  The bandwidth that is allocated for non-priority traffic should take into account the bandwidth that is reserved by the **police** *bps* command for the real-time class.

  Workaround: Remove and reapply the **service-policy out** command to the multilink interface.

- CSCee30116

  Symptoms: CNS config notify events may stop coming.

  Conditions: This symptom is observed when the **cns config notify diff** command is enabled and when other CNS configuration agents are configured.

  Workaround: Enter the **no cns config notify** command followed by the **cns config notify diff** command.

- CSCee32577

  Symptoms: A Cisco 10720 router uses the size of the Ethernet packet frame plus the 20-byte preamble interpacket gap when calculating shaping rate. Therefore, the shaped rate is lower than what your would expect if you perform the calculation based only on the Ethernet frame size.

  Conditions: This symptom occurs when a shape statement is configured in a policy map.

  Workaround: There is no workaround

  Further Problem Description: Because the police statement in the Modular QoS CLI only uses the Ethernet frame size, the shape rate and police rate are inconsistent.

- CSCee34094

  Symptoms: A standby RP keeps crashing.

  Conditions: This symptom is observed when both the **snmp-server community** *string* **rw** command and the **snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart** command are configured.

  Workaround: Remove the **snmp-server community** *string* **rw** command from the startup configuration before rebooting the router. When the router has booted, reenter the **snmp-server community** *string* **rw** command.

- CSCee36744

  Symptoms: An RP may crash when you add or remove a channel group to or from a 4-port ISE Gigabit Ethernet line card or when you reload microcode onto the line card on which channel group members are configured.

Conditions: This symptom observed on a Cisco 12000 series when there are link-bundle subinterfaces configured on the 4-port ISE Gigabit Ethernet line card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed63480. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: There is no workaround.

- CSCee40349

  Symptoms: Cisco 12816 and 12810 routers need to have specific MBSU 5v and on- board 5v thresholds other than the values in the legacy system. Otherwise, there may be error messages in the console logs that complain that the voltages are abnormal.

  Conditions: This symptom is observed on Cisco 128xx series routers.

  Workaround: The **no show environment** command can be configured, but only if this problem is seen.

- CSCee41728

  Symptoms: Some voltage threshold levels may not be set correctly and may cause a line card to power down without any warning messages if the voltage drops below 3v. Note: There has been no reports of this happening yet.

  Conditions: This symptom is observed on Cisco 12000 series routers.

  Workaround: The **no show environment** command can be configured, but only if this problem is seen.

- CSCee42198

  Symptoms: Engine 4+ loadsharing does not work correctly in a VPN imposition situation. The problem is not seen with Engines 0, 2 and 3.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S when traffic enters on a VRF interface and is loadshared over four links to the core. Traffic is loadshared over only two of the four links.

  Workaround: Use three-path loadbalancing.

- CSCee43855

  Symptoms: Starting with Cisco IOS Release 12.0(26)S, the Cisco 10720 router supports the IPv6 ACL feature. The IPv6 packets are corrupted (including the IPv6 header) for the following scenario: For a packet in 6PE decapsulation case (MPLS to IPv6), if output ACLs are applied at the output interface and these ACLs are long enough to require a second PXF pass (known as output ACL split case), then the outgoing IPv6 packet is corrupted.

  Conditions: This symptom is observed on Cisco 10720 routers that are running Cisco IOS Release 12.0(26)S or later releases.

  Workaround: There is no workaround.

- CSCee55457

  Symptoms: When the channel-group is removed on the controller, class-default queue gets stuck on next time slot/channel (removed channel+1).

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 24-port channelized E1/T1 line cards with high traffic rate on removed channel.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCee57438

  Symptoms: The second port pair (interface SRP x/1) of an Engine 4+ 4-port OC-48 DPT line card is unable to forward traffic (including pings) at layer 3. The first port is also damaged (interface SRP x/0); a portion of its forwarding capabilities is damaged. The layer 2 SRP protocol operates correctly.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(27)S1 and does not require any specific trigger: the symptom is always there.

  Workaround: There is no workaround.

- CSCin41269

  Symptoms: A controller of an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) may fail to come up after the router has booted up.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-8TE1+. The symptom is platform independent and port adapter dependent.

  Workaround: Enter the **shutdown** controller configuration command followed the **no shutdown** controller configuration command on the affected controller.

  Alternate Workaround: Enter the **clear counters** user EXEC or privileged EXEC command on the affected interface of the PA-MC-8TE1+.

- CSCin52138

  Symptoms: When flaps occur on an Inverse Multiplexing over ATM (IMA) group interface on which the Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: VC Mode feature is configured, input packets may be switched via Cisco Express Forwarding (CEF).

  Conditions: This symptom is observed on a Cisco 7500 series that has an IMA group interface that is configured on a Versatile Interface Processor (VIP).

  Workaround: Perform an online insertion and removal (OIR) of the VIP.

- CSCin61140

  Symptoms: A line card reloads continuously after an OIR.

  Conditions: This symptom is observed when the line card has MFR and a service policy configured.

  Workaround: Remove the service policy before performing an OIR.

- CSCin62978

  Symptoms: A FlexWAN, enhanced FlexWAN, or Versatile Interface Processor that has a PA-MC-E3 or PA-MC-T3 installed may crash.

  Conditions: This symptom is observed under rare conditions in a stress situation with dFLI and dCRTP configured.

  Workaround: There is no workaround.

- CSCin66542

  Symptoms: The line protocol on a T1 of a T3 controller in a PA-MC-2T3+ port adapter may stay in the down state even when looped.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series.

  Workaround: There is no workaround.

- CSCin72219

  Symptoms: If you enter the **shutdown** command followed by the **no shutdown** command on an interface, traffic that congests the interface may cause the router to crash.

Conditions: This symptom is observed when a policy is attached to the interface.

Workaround: There is no workaround.

- CSCin74347

  Symptoms: Outbound security ACLs are not applied properly on Cisco10000 series routers.

  Conditions: This symptom is observed on all Cisco IOS Release 12.0 S images that contain the fix for CSCed72686.

  Workaround: There is no workaround.

- CSCuk48013

  Symptoms: A Cisco 7500 series router that is running 12.0S may drop traffic to a static route after a microcode reload. The symptom may also occur in other releases.

  Conditions: Traffic loss will occur for static routes to /32 prefixes that are attached to an interface, that is, the **ip route** *prefix mask interface-type interface-number* command is enabled.

  Workaround: Disable Cisco Express Forwarding (CEF) by entering the **no ip cef** command. Then, reenable CEF by entering the **ip cef distributed** command.

- CSCuk48808

  Symptoms: Following an OIR, the **show ip cef inconsistency now** command may report an inconsistency between an RP and a VIP. There are no inconsistencies reported on the VIP itself.

  Conditions: This symptom is observed on Cisco 7500 series that runs Cisco IOS Release 12.0 S.

  Workaround: There is no workaround.

- CSCuk48818

  Symptoms: On a Cisco 12000 ATM ISE line card, shaping resources may be used up after different policy-maps are attached and then removed from a VC many times.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: Microcode reload the line card.

TCP/IP Host-Mode Services

- CSCeb21552

  Symptoms: The following error message may be displayed when a router receives a connection request on command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports:

  ```
  %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.2.2
  ```

  Conditions: This symptom is observed on a Cisco router that has the remote shell (rsh) disabled.

  Workaround: Filter the traffic that is destined for command-shell (TCP, 514) and Kerberos-shell (kshell) (TCP, 544) ports.

  First, enter the **show ip interface brief** EXEC command to display the usability status of interfaces that are configured for IP. The output may look like the following:

  ```
  Interface IP-Address OK? Method Status Protocol Ethernet0/0 172.16.1.1 YES NVRAM up
  up Ethernet1/0 unassigned YES NVRAM administratively down down Serial2/0 192.168.2.1
  YES NVRAM up up Serial3/0 192.168.3.1 YES NVRAM up up Loopback0 10.1.1.1 YES NVRAM up
  up
  ```

  Then, create the following access control list (ACL) for the router and apply this ACL to all interfaces that are enabled with the **ip access-group 177 in** router configuration command:

  ```
  access-list 177 deny tcp any host 172.16.1.1 eq 514
  ```

```
access-list 177 deny tcp any host 172.16.1.1 eq 544
access-list 177 deny tcp any host 192.168.2.1 eq 514
access-list 177 deny tcp any host 192.168.2.1 eq 544
access-list 177 deny tcp any host 192.168.3.1 eq 514
access-list 177 deny tcp any host 192.168.3.1 eq 544
access-list 177 deny tcp any host 10.1.1.1 eq 514
access-list 177 deny tcp any host 10.1.1.1 eq 544
access-list 177 permit ip any any
```

Wide-Area Networking

- CSCec83030

  Symptoms: A parity error on a Versatile Interface Processor (VIP) card may cause other VIPs to go to a wedged state.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCed52817

  Symptoms: Even though you remove the **frame-relay fragment** command from an active RP, the command may be back in the configuration after a switchover.

  Conditions: This symptom is observed on a Cisco 10000 series, but not on a Cisco 7500 series and Cisco 12000 series.

  Workaround: After you have removed the **frame-relay fragment**, **frame-relay interface-queue**, or **frame-relay ip rtp** command from a map class on the active RP, reset the standby RP to enable the standby RP to read the configuration changes.

Resolved Caveats—Cisco IOS Release 12.0(27)S1

Cisco IOS Release 12.0(27)S1 is a rebuild of Cisco IOS Release 12.0(27)S. The caveats listed in this section are resolved in Cisco IOS Release 12.0(27)S1 but may be open in previous Cisco IOS releases. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCed21186

  Symptoms: Incorrect “output IFMIB” counters are observed on the main interface.

  Conditions: This symptom has been observed on a Cisco 7500 series router running Cisco IOS Release 12.0(25)S1 when an 802.1q VLAN is configured with Committed Access Rate (CAR). The “output CLI” and “input SNMP/CLI” counters are correct.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCed47550

  Symptoms: BGP Policy Accounting information is not available via SNMP for 802.1Q VLAN subinterfaces.

  Conditions: This symptom is observed on Cisco 12000 and 7500 series routers.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed35907

  Symptoms: When the following CLI sequence is configured, the router may run into a race condition and crashes:

  ```
  router ospf 100
  router ospf 1000 vrf <vrf_name>
  ```

  then

  ```
  no router ospf 100
  router ospf 1000
  no router ospf 1000
  ```

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.3(4)T and later releases. A configuration script with the above CLI sequence is run on the router.

  Workaround: There is no workaround.

- CSCed41323

  Symptoms: A Cisco router with a label switched path (LSP) tunnel on which Fast ReRoute (FRR) is enabled and active may stop refreshing the Resource Reservation Protocol (RSVP) state when the refresh updates are received via RSVP summary refresh messages. This situation causes the RSVP to time out and the LSP tunnel to be torn down.

  Conditions: This symptom is observed on a Cisco router that does not transmit RSVP messages for LSP tunnels on which FRR is enabled and active via message IDs. The symptom does not occur when FRR is enabled but not active.

  A peer router that runs software other than Cisco IOS software may continue to send RSVP messages with messages IDs that request an acknowledgment. The Cisco router does acknowledge these message IDs, causing the peer router to start sending RSVP summary refresh messages to refresh the RSVP state. The Cisco router ignores the message IDs that are contained in these RSVP summary refresh messages and does not refresh the RSVP state.

  Workaround: There is no workaround.

- CSCed60289

  Symptoms: IP background process is sluggish.

  Conditions: This symptom occurs when many interfaces go down at the same time.

  Workaround: There is no workaround.

Miscellaneous

- CSCeb22276

  Symptoms: Some Simple Network Management Protocol (SNMP) packets may linger in the input queue while they are processed. However, the packets do exit the queue on their own without any intervention from the user. This fix allows these packets to be removed from the queue more quickly.

  Conditions: This symptom is observed on a device that runs Cisco IOS software and that supports SNMP operations. In addition, the SNMP request must contain a valid community string.

  Workaround: Protect the SNMP community strings with good password management. Permit SNMP traffic only from trusted devices.

- CSCec07354

  Symptoms: On dual Performance Route Processors (PRPs), the secondary PRP does not boot up. When logging into the card, it is in the ROMmon state.

  Conditions: This symptom occurs when upgrading to Cisco IOS Release 12.0(15)S1.

  Workrooms: Boot up the card manually with the **boot** command on the Common prompt.

- CSCec63687

  Symptoms: An E3 4xOC12 channelized line card keeps resetting.

  Conditions: This symptom is observed under load sharing between a POS channel interface and a regular POS interface.

  Workrooms: There is no workaround.

- CSCec77256

  Symptoms: Basic VPN with SRP Dense (E4P) links fail the ping test.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running the Cisco IOS Release 12.0 S image gsr-p-mz.

  Workaround: There is no workaround.

- CSCed02802

  Symptoms: A 1-port 10-Gigabit Ethernet line card may generate pause frames under an inbound heavy load if there is a bottle neck in the router, for example an egress line card. The pause frames may cause FCS errors at the remote end device.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(25)S2.

  Workaround: There is no workaround.

- CSCed03096

  Symptoms: Shutting down the loopback 0 causes the 3xGigabit Ethernet (engine 2) line card that is configured with EoMPLS and VPN to fail.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed06014

  Symptoms: On a Cisco router, IPv6 traffic is counted under IPv4 counter on the Engine 4 POS line cards on the egress side when using the **show interface** *number* [**accounting**] command.

  Conditions: This symptom is observed on a Cisco 12000 series router.

Workaround: There is no workaround.

- CSCed08696

  This umbrella caveat affects the behavior of path triggers, and of Automatic Protection Switching (APS) with PPP and Frame Relay (FR) encapsulation.

  - CSCec70879:

  Symptoms: Cisco 12000 series POS APS interfaces do not permit the configuration of path trigger specifications on APS interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

  - CSCdu45201:

  Symptoms: When the **encapsulation ppp** interface configuration command is configured with Cisco 12000 series Packet-over-SONET (POS) APS interfaces, some APS operations may result in inappropriate protocol state. This may stop all traffic flow through the APS pair or duplicate all packets.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

  - CSCec72228:

  Symptoms: When the **encapsulation frame-relay** interface configuration command is configured with Cisco 12000 series POS APS interfaces, some APS operations may result in interfaces that have been selected by APS being set to “protocol down” by FR. This behavior can result in the loss of all traffic over the APS pair.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed14064

  Symptoms: On a Cisco router that is configured with LLQ, there is queueing on the real time queue.

  Conditions: This symptom is observed on a Cisco 10000 ESR that is configured with LLQ.

  Workaround: There is no workaround.

- CSCed20042

  Symptoms: A Cisco router may unexpectedly reload if IPv6 encounters a routing loop, and IPv6 CEF is enabled.

  Conditions: This symptom occurs under the following conditions:

  – IPv6 must be enabled
  – IPv6 CEF must be enabled
  – The IPv6 RIB must have recursive entries that form a loop, for example:

```
Router# show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
B   ::/0 [200/0]
     via 2::2
```

```
C   1::/64 [0/0]
     via ::, Ethernet0/0
L   1::2/128 [0/0]
     via ::, Ethernet0/0
C   2::/64 [0/0]
     via ::, Ethernet1/0
L   2::1/128 [0/0]
     via ::, Ethernet1/0
B   2001::/16 [200/0]
     via 2002::1
B   2002::/16 [200/0]
     via 2001::1
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Note that 2001::/16 and 2002::/16 results in a recursion loop because 2001::/16 is accessible via 2002::/16 and 2002::/16 is accessible via 2001::/16.

Workaround: Disable IPv6 CEF using the global configuration command **no ipv6 cef**.

- CSCed23828

  Symptoms: L2 fragmentation does not happen for packets greater than the network Maximum Transmission Unit (MTU). Packets are dropped.

  Conditions: This symptom occurs when distributed Cisco Express Forwarding (dCEF) is enabled on RSP.

  Workaround: User can either turn dCEF off or configure MTU, which is equal to the network MTU on the customer edge (CE) routers.

- CSCed26664

  Symptoms: The output packet counters on an interface may be incorrect. Depending on the Cisco IOS release, they may show either a very large value or zero.

  Conditions: The output packet counters get corrupted by clearing the interface counters followed by reloading the PXF microcode. The commands are the **clear counters** command followed by the **microcode reload pxf** command.

  Workaround: Issue another **clear counters** command.

- CSCed29519

  Symptoms: An Engine 4+ GE line card stops forwarding Multiprotocol Label Switching (MPLS) VPN traffic.

  Conditions: This symptom occurs after Cisco Express Forwarding (CEF) on the line card is cleared.

  Workaround: Enter the **shut** command followed by the **no shut** command on the line card.

- CSCed29776

  Symptoms: **traffic-shape** disappears from the running- configuration after HA switchover and it is not possible to re-configure it on the newly active route processor.

  Conditions: If **traffic-shape** is configured on an Engine 4+ interface on a Cisco 12000 series router with multiple route processors installed and HA switchover occurs, **traffic-shape** may disappear from the running-configuration. It is not possible to reconfigure it in the running-configuration.

Workaround: Reload the router and reconfigure **traffic- shape**.

- CSCed33627

  Symptoms: A 3-port Gigabit Ethernet (GE) line card may show BMA error, then run error recovery.

  Conditions: This symptom is observed on a Cisco 12008/40 router that is running Cisco IOS 12.0(23)S5. It is configured as an MPLS inter-AS ASBR. It is also configured as a PE router. When entering the **shut** command followed by the **no shut** command on a POS interface on a 8POS LC, the 3GE LC will show BMA error.

  Workaround: There is no workaround.

- CSCed35573

  Symptoms: Ping does not go through for large packet sizes.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed39106

  Symptoms: Removal of the primary CSC from a Cisco 12816 router (when all 5 fabric cards are present in the router), stalls the active RP for about 10 minutes and brings down standby RP to ROMMON prompt.

  Conditions: This symptom is observed on a Cisco 12816 router.

  Workaround: Do not do primary CSC OIR.

- CSCed40933

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory, which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml.

- CSCed42587

  Symptoms: When sending 10 packets from AGT-SRC to AGT-Dest with TTL set to 3 on all packets, the first packet is dropped.

  Conditions: This symptom occurs under the following conditions:

  - Applies only to E2 LCs.

  - Interface with ACL rule with the “log” option

  - Packets with TTL of 3

  Workaround: Remove the “log” option from the ACL rule.

- CSCed43228

  Symptoms: On a Cisco 12000 series router with 2 GRPs which support SSO mode (Cisco IOS Release 12.0(24)S and later), when any Engine3 (E3 aka ISE) card is inserted after bringing up both GRPs in SSO mode, the applied service policy which has WRED configured on this interface, does not sync with standby GRP.

  Conditions: The problem only happens for any E3 card that was not in the chassis when the secondary RP booted. This will be the case when adding a new E3 LC to an already running system and configuring it for the first time. E3 cards that were in the chassis by the time the secondary RP finished booting will not exhibit this behavior.

Workaround: Reload the secondary RP.

- CSCed43829

  Symptoms: Random Early Detection maintains an average length of the outbound queue of a class of traffic, and randomly discards newly arriving packets when the average falls within the configured range. A Cisco 10000 series router, that is running any of the identified Cisco IOS software, contains an error in the average queue length computation which makes Random Early Detection too sensitive to the instantaneous queue length.

  Conditions: This problem is seen on the Cisco 10000 series routers that are running all Cisco IOS releases identified in this report.

  Workaround: There is no workaround.

- CSCed46856

  Symptoms: Most multicast traffic is dropped if ingress interface is a E4+ and netflow is configured.

  Conditions: This symptom occurs when multicast traffic is forwarded down shared tree, for example, forwarded by (*, g); ingress interface is E4+; and netflow is configured.

  Workaround: Either unconfigure netflow or disable SPT threshold to move to the shortest path tree.

- CSCed47409

  Symptoms: In Cisco IOS software that is running Multiprotocol Label Switching (MPLS), a router may reload after accessing a freed Label Information Base (LIB) entry. When the symptom occurs, an error message similar to the following is likely to precede the reload:

  %TIB-3-LCLTAG: 10.10.10.10/10.10.10.10, tag advert; unexpected tag state=13

  Conditions: This symptom is observed when a very uncommon timing of a Label Distribution Protocol (LDP) events occurs. The symptom may occur with LDP or Tagswitching Distribution Protocol (TDP).

  Workaround: There is no workaround.

- CSCed49733

  Symptoms: The Cisco 10720 microcode will be reloaded upon reception of certain malformed MPLS packets.

  Conditions: An MPLS packet where the topmost label is an MPLS Aggregate Label (for either IPv4 or IPv6) and this label does not have the EOS bit set (that is, it is not the only label) will cause the reload.

  Workaround: There is no workaround

  Further Problem Description: This should be an extremely rare situation as such packets are not allowed in MPLS, that is, IPv4/IPv6 aggregate MPLS labels must always be the only label on the received label stack and therefore they must always have the EOS bit set. Reception of such a packet implies that some other network element has generated an invalid MPLS packet.

- CSCed50426

  Symptoms: All multicast packets are dropped with a VRF-lite configuration.

  Conditions: This symptom occurs when MVPN is set up in a VRF-lite configuration.

  Workaround: There is no workaround.

- CSCed50510

  Symptoms: An IPC crash may be seen on a standby RP while upgrading from the gsr-p-mz image of Cisco IOS Release 12.0(25)S1 to the gsr-p-mz image of Cisco IOS Release 12.0(27)S. Tracebacks and error messages "%IPCGRP-3-UNKNOWNCMDMSG:" and "%IPCGRP-3-SYSCALL:" may be seen as well.

  Conditions: This symptom is observed on a Cisco 12416 router when following the recommended upgrade procedure.

  Workaround: There is no workaround.

- CSCed51139

  Symptoms: A Cisco 12000 series router with an HA configuration (dual RP redundancy) and with GE line cards which are using channel groups, might not be pingable after a redundancy switchover. From the interface, the directly connected device can be pinged, but from the same device, the interface cannot be successfully pinged.

  Conditions: The problem is specific to a Cisco 12000 series router that is running Cisco IOS 12.0 S. The router must have an HA configuration (dual RPs). Also, channel groups must be configured (note: even if the channel groups are not assigned to a particular Gige interface, the problem can still occur). Finally, a link flap needs to occur on the channel group interface before the redundancy switchover is done to bring on the problem.

  Workaround: Enter the **shut** command followed by the **no shut** command on the interface. Further Problem Description: The group channel feature is new and was released for the first time in Cisco IOS Release 12.0(26)S1 so that is where the exposure is.

- CSCed51610

  Symptoms: The Cisco 12000 series router Engine 4+ is unable to originate ICMP echo reply packets. ICMP packets transiting the router are correctly transmitted.

  Conditions: This symptom occurs when **rate-limit**, MQC **set**, or MQC **police** commands are configured on the interface in the **output** direction.

  Workaround: There is no workaround.

- CSCed54236

  Symptoms: A Cisco router reloads due to memory allocation problem when per packet load balancing is changed to default CEF load balancing.

  Conditions: This symptom is observed on a Cisco 7200 series router with PA-4T serial adapter when "service-policy output <name>" is applied to that interface. Problem is observed in Cisco IOS Release 12.0(26)S1 and Release 12.0 (27)S.

  Workaround: Use per-packet load balancing or remove "service-policy output <name>" or replace adapter with PA-4T+.

- CSCed68450

  Symptoms: When removing VP and VC L2 connection on a 4xOC12 E3 ATM, you get a SAR free channel error message. The connection cannot be set up again properly. Cells are lost if traffic is sent on this connection.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: There is no workaround.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

- CSCed68763

  Symptoms: Engine 2 line cards may fail upon clearing BGP peers.

  Conditions: This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(27)S.

  Workaround: There is no workaround.

- CSCed72764

  Symptoms: Using the images, gsr-p-mz.120-27.2.S1, TE tunnel(s) fail to switch back to the explicit path option.

  Conditions: This symptom is observed on a Cisco 12000 series router.

  Workaround: Continue to work either in the explicit path or in the dynamic path without shutting the link. Such a scenario is highly unlikely.

- CSCin66535

  Symptoms: On a Cisco 7500 series router, after a RPR, RPR-plus or SSO switchover, the router may display the following messages:

  ```
  %RSP-3-RESTART: cbus complex
  ```

  This will be followed by the reload of all line cards in the router.

  It will be followed by the messages:

  ```
  HA-2-NO_QUIESCE: Slot <slot#> did not quiesce, it will be disabled and then reloaded.
  ```

  Conditions: This problem happens on a Cisco 7500 series router that is running Cisco IOS Release 12.0S and occurs after an RPR, RPR-plus, or SSO switchover. Similar symptoms can be observed if **service single-slot-reload-enable** is not configured on the router. But in that case, the cbus complex message will follow the HA-2-NO_QUIESCE error message(s).

  Workaround: There is no workaround.

- CSCuk48156

  Symptoms: Failover boot commands from slot to disk results in endless loop. If the router does not find the image in slot0, it will not be able to properly switch to the next image in disk1.

  Conditions: This symptom occurs when slot0 holds linear flash and disk1 holds ATA disk.

  Workaround: While being in a loop in the console connection, press control plus return, type and send break till the loop stops.

Resolved Caveats—Cisco IOS Release 12.0(27)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(27)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdw85004

  Symptoms: The Response Time Reporter (RTR) uses random User Datagram Protocol (UDP) ports to respond to Service Assurance Agent (SAA) probes.

  Conditions: This symptom is observed on a Cisco router.

  Workaround: There is no workaround.

- CSCea74631

  Symptoms: A Route Switch Processor (RSP) that is acting as a slave may have complete packet switching activity interrupted for several minutes. This situation may cause the RSP to permanently pause.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(12d).

  Workaround: There is no workaround.

- CSCeb42542

  Symptoms: The CPU utilization of a Cisco 7500 series Versatile Interface Processor (VIP) may reach 100 percent when the rate of the incoming traffic exceeds the bandwidth of the egress interface.

  Conditions: This symptom is observed only with local switching, that is, it is observed only with traffic that enters through one interface of the VIP and that leaves through another interface of the same VIP.

  Workaround: Reload the affected VIP.

- CSCeb43981

  Symptoms: When High System Availability (HSA) is configured, the standby Route Switch Processor (RSP) may not become active when the primary RSP reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S or Release 12.2 S when you configure the primary RSP in slot 2 and the standby RSP in slot 3.

  Workaround: Configure the secondary RSP in slot 2 by entering the **slave default-slot 2** global configuration command. The symptom does not occur when you configure the secondary RSP in slot 2 and the primary RSP in slot 3.

- CSCeb51200

  Symptoms: If a switch has the nvram:ifIndex-table file in the wrong format, there is a problem at bootup. The following message is printed when this problem exists:

  ```
  SYSTEM INIT: INSUFFICIENT MEMORY TO BOOT THE IMAGE!
  ```

  Conditions: This problem is observed in Cisco IOS Release 12.1(13)EW and Release 12.1(19)EW.

  Workaround: Do not create a file called ifIndex-table in NVRAM.

Note: If the nvram:ifIndex-table file is created by software (because of the snmp-server ifindex persist configuration command), there should be no problem in the format of the file. There is no need to delete the file if you see it and if the switch is running and booting smoothly.

- CSCeb66973

  Symptoms: A Cisco router or switch may reload when it attempts to read the ifIndex information from an NVRAM file during the bootup process.

  Conditions: This symptom is observed when the NVRAM file is corrupt.

  Workaround: Disable the ifIndex persistence.

- CSCec10125

  Symptoms: A Cisco router may go into a continuous loop if the image in the flash memory is bad, missing, or has the incorrect name.

  Following is the error message output of a test performed with an incorrect file name (a "/" was added to the image name).

```
++++++++++++++ System Bootstrap, Version 12.0(10r)S1, RELEASE SOFTWARE (fc1) Copyright
(c) 2000 by cisco Systems, Inc.

SLOT 7 RSP is system master RSP8 platform with 262144 Kbytes of main memory

open(): Open Error = -9 loadprog: error - on file open boot: cannot load
"slot0:/rsp-jsv-mz.121-14.E4"

System Bootstrap, Version 12.0(10r)S1, RELEASE SOFTWARE (fc1) Copyright (c) 2000 by
cisco Systems, Inc.

SLOT 7 RSP is system master RSP8 platform with 262144 Kbytes of main memory

open(): Open Error = -9 loadprog: error - on file open boot: cannot load
"slot0:/rsp-jsv-mz.121-14.E4"

System Bootstrap, Version 12.0(10r)S1, RELEASE SOFTWARE (fc1) Copyright (c) 2000 by
cisco Systems, Inc.

SLOT 7 RSP is system master RSP8 platform with 262144 Kbytes of main memory

open(): Open Error = -9 loadprog: error - on file open boot: cannot load
"slot0:/rsp-jsv-mz.121-14.E4"
```

  Conditions: This symptom is observed on a Cisco 7500 series router with a Route Switch Processor 8 (RSP8) that is running a bootstrap image of Cisco IOS Release 12.0(10r)S1.

  Workaround: Perform a remote break on the console port of the router, and enter the **boot** command in rommon mode to use the correct Cisco IOS software image.

- CSCin58957

  Symptoms: A Cisco 7500 series router may not generate Simple Network Management Protocol (SNMP) ENVMIB traps during the online insertion and removal (OIR) of a power supply or fan module.

  Conditions: These symptoms have been observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0(24)S or later.

  Workaround: There is no workaround.

Interfaces and Bridging

- CSCea59948

  Symptoms: A cbus complex may be observed on a Cisco router when the following message appears on the serial interface:

```
%RSP-3-RESTART: interface Serial8/1/0/23:23, not transmitting
```

Conditions: This symptom is observed on a Cisco 7500 series router when Multilink PPP (MLP) is configured on the serial interface and distributed Cisco Express Forwarding (dCEF) switching is enabled.

Workaround: There is no workaround.

- CSCea66198

  Symptoms: A Cisco 7500 series router may encounter a bus error when applying a crypto map on an FDDI interface.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(11)T2, Release 12.2(13)T1, or Release 12.2(13a). The symptom may also occur in other releases such as Release 12.0 S.

  Workaround: There is no workaround.

- CSCeb38393

  Symptoms: A Cisco 7500 series may generate the following message on its console:

  ```
  %VIP-3-BADMALUCMD: Unsupported MALU command 81/82
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(23)S1.

  Workaround: There is no workaround.

- CSCeb59227

  Symptoms: The ifOutUcastPkts, ifOutOctets, and ifHCOutOctets Simple Network Management Protocol (SNMP) counters of a Fast Ethernet subinterface may not be incremented.

  Conditions: This symptom is observed on a Cisco 7500 series when traffic is received from a serial interface in a Multiprotocol Label Switching (MPLS) network and when the Fast Ethernet subinterface is configured for dot1q encapsulation.

  Workaround: There is no workaround.

- CSCec26643

  Symptoms: Packet-over-SONET (POS) interfaces on a 1-port POS OC-3c/STM-1 port adapter (PA-POS-OC3) that is installed in a Cisco 7200 series router that runs Cisco IOS Release 12.2(14)S3 may stop transmitting packets. The output packets counter stops incrementing.

  Conditions: This symptom is observed when you reload the router with a queueing configuration on the POS interfaces.

  Workaround: Remove the queueing configuration before you reload the router. Reapply the queueing configuration after the router has booted up.

- CSCec79579

  Symptoms: A FlexWAN module may reload unexpectedly while the switch or router boots up and brings up the modules and port adapters.

  Conditions: This symptom is observed when a 1-port T3 serial port adapter (PA-T3) is installed in the FlexWAN module.

  Workaround: There is no workaround.

- CSCin38177

  Symptoms: When a router boots up, a FlexWAN module that is configured with a serial T3 port adapter may come up and may reload immediately.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series or Cisco 7600 series.

Workaround: There is no workaround.

- CSCin53729

  Symptoms: Poor performance is observed when the ATM packed cell relay feature is configured in virtual path (VP) mode.

  Conditions: This symptom is observed when a large number of VPs are configured on a PA-A3 port adapter and the packed cell relay feature is enabled on all of the VPs.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCdw75860

  Symptoms: There is inoperability between Cisco IOS Release 12.2 and earlier releases when you configure an invalid encrypted password for Message Digest 5 (MD5) authentication for Open Shortest Path First (OSPF). An error message similar to the following is displayed to warn the user of this invalid password.

  ```
  router(config-if)# ip ospf message-digest-key 111 md5 7 xxxxxx
  OSPF: Invalid encrypted password: xxxxxx
  An already encrypted password should have been entered.
  ```

  Conditions: This symptom is observed on all Cisco platforms.

  Workaround: There is no workaround.

- CSCdy07364

  Symptoms: If you provide routed bridge encapsulation (RBE) with a policy map as in the following example, line card online insertion and removal (OIR) events occur.

  Example:

  ```
  access-list 10 permit any

  route-map <name> permit 10
  match ip address 10
  set ip next-hop x.x.x.x

  int atm5/0/0.1 point
   ip unnumbered gig1/0/0
   ip policy route-map badboy
   atm route-bridged ip
   range pvc 0/100 0/2000
   atm route-bridged ip
   range pvc 0/100 0/2000
  ```

  Conditions: This symptom is observed on a Cisco 10000 series router.

  Workaround: Remove any **ip policy route-map** statements from the policy map.

- CSCea46372

  Symptoms: A Cisco router may reload when you add Border Gateway Protocol (BGP) neighbor statements to the configuration.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S or Release 12.2 S when BGP neighbors are added by using a script that adds the BGP neighbors at a much faster rate than manual addition, and when a large BGP table is already present on the router before the script adds the BGP neighbors.

  Workaround: There is no workaround.

- CSCea64025

  Symptoms: A “Path Tear” message may be ignored for an old label switch path (LSP) at a merge point, and the LSP is not torn down.

  Conditions: This symptom is observed when a protected interface comes up and a new LSP is generated.

Workaround: There is no workaround. Note that the old LSP times out after five minutes.

- CSCea66336

  Symptoms: A Cisco router may be unable to set up a Frame Relay or an ATM permanent virtual connection (PVC). When you enter the **debug ip rsvp traffic-control** EXEC command, the following message is displayed:

  ```
  RSVP-TC: Unable to determine resource provider for tcsb
  ```

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(15)T.

  Workaround: There is no workaround.

- CSCea81029

  Symptoms: A Cisco router may reload unexpectedly when you enter a **show** command that is related to IP multicast.

  Conditions: This symptom is observed on a Cisco router that has remained at the "more" prompt for a long period of time.

  Workaround: There is no workaround.

- CSCeb27742

  Symptoms: A Cisco router with a Border Gateway Protocol (BGP) system may lose the address family's use of aggregate routes after the router reloads. The aggregate routes are moved from the VPN routing/forwarding (VRF) address family and appear under the global IP version 4 (IPv4) address family. When the router reloads, the console displays the following error messages:

  ```
  exit-address-family ^
    % Invalid input detected at "^" marker.
  exit-address-family ^
    % Invalid input detected at "^" marker.
  exit-address-family ^
    % Invalid input detected at "^" marker.
  ```

  The above symptom is only one of the possible symptoms. Support for the **auto-summary** router configuration command and the **default-information originate** router configuration command has been removed from some of the address families as a result of the caveat CSCdx14351 without providing support to accept these commands silently when being booted with a configuration from a prior Cisco IOS release. The presence of the unsupported commands in address families like Virtual Private Network version 4 (VPNv4) and IPv4 Multicast (MCAST) causes the command-line interface (CLI) to go out of the address family submode and apply these commands to the v4 address family, which results in unpredictable behavior.

  Conditions: This symptom is observed on all Cisco platforms that are running Cisco IOS Release 12.2(16.4)T or Release 12.3 T. The symptom is not observed in Cisco IOS Release 12.3.

  Workaround: Reenter the configuration that was present before the router reloaded.

- CSCeb42893

  Symptoms: A Cisco 7200 series may select the best path inconsistently.

  Conditions: This symptom is observed on a Cisco 7200 that runs Cisco IOS Release 12.0(26)S when the **bgp deterministic med** router configuration command, the **bgp always-compare-med** router configuration command, or both commands are configured to determine the best path.

  Workaround: Use other commands or methods to determine the best path.

- CSCeb53391

  Symptoms: Border Gateway Protocol (BGP) may not advertise all routes to a peer.

  Conditions: This symptom is observed when the peer comes up after all other peers of an update group have converged.

  Workaround: There is no workaround.

- CSCeb53542

  Symptoms: An inconsistency between the Cisco Express Forwarding (CEF) table and the Address Resolution Protocol (ARP) table may cause CEF entries to be removed and then recreated at random times. This situation, in turn, may cause unicast packet loss for the affected entry or entries.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series that is configured with three VLAN interfaces and that directly connect to a Layer 2 port-channel interface. This port-channel interface connects via a trunk to an access-layer device.

  When you enter the following EXEC commands on components of the Cisco Catalyst 6000 series, the output does not show entries for the affected addresses:

  - **show ip cef** on the Multilayer Switch Feature Card (MSFC)
  - **show ip cef on the Supervisor**
  - **show ip cef on the Distributed Forwarding Card (DFC)**
  - **show mls cef on the Supervisor**
  - **show mls cef on the DFC**

  Workaround: Configuring the ARP timeout to a time on a 60-second boundary may resolve this issue in some cases. For example, when you enter the **arp timeout 270** interface configuration command, the symptom occurs, but when you enter the **arp timeout 300** interface configuration command, the symptom does not occur.

  For cases where configuring the ARP timeout to a time on a 60-second boundary does not resolve the issue, upgrading is the only solution.

- CSCeb57086

  Symptoms: A Cisco 10000 series that is configured with two Performance Routing Engine 1 (PRE-1) processors may stop functioning as a redundant system.

  Conditions: This symptom is observed when you enter the **bgp upgrade-cli** router configuration command.

  Workaround: Reload the standby PRE-1.

- CSCeb59623

  Symptoms: A Cisco router may pause indefinitely or reload when you enter the **debug ip rsvp summary-refresh** privileged EXEC command and there is a large number of Resource Reservation Protocol (RSVP) flows, for example, when Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switched paths (LSPs) are configured.

  Conditions: This symptom is observed even when you have configured an access control list (ACL) that is supposed to reduce the number of debugs to a single LSP. The symptom occurs because the ACL does not function for some of the summary refresh debugs.

  Workaround: Do not enter the **debug ip rsvp summary-refresh** privileged EXEC command when a large number of flows is active.

- CSCeb60432

  Symptoms: If an object in a Resource Reservation Protocol (RSVP) reservation (RESV) refresh changes in relation to the previous refresh, a debug message may be generated that is not subjected to an access control list (ACL). When many flows or label switched paths (LSPs) are active on a router, this situation may cause so much debug output that the router may pause indefinitely or reload.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(25)S when the **debug ip rsvp filter** privileged EXEC command is configured to reduce the number of debugs on a subset of RSVP flows or Multiprotocol Label Switching (MPLS) traffic engineering LSPs and when you also configure the **debug ip rsvp resv** privileged EXEC command. The ACL that is enabled with the **filter** keyword of the **debug ip rsvp filter** privileged EXEC command may not function for one debug message.

  Workaround: Do not configure the **debug ip rsvp resv** privileged EXEC command when there are many flows on the router.

- CSCeb63120

  Symptoms: When refresh reduction is enabled and a Cisco router has been operational for a long time, valid Resource Reservation Protocol (RSVP) messages that are received from a neighbor may be dropped when the message IDs have cycled through the entire number space once (that is, from 0 to 4,294,967,295) and then progressed up to 2,147,483,648 (0x80000000).

  Conditions: This symptom is observed when a message ID number space begins at zero, increases up to 4,294,967,295 (32 bits), but then does not properly wrap back to zero, causing message IDs greater than 2,147,483,648 to be out of sequence, and to be dropped.

  Note that a neighboring router is able to send Message IDs and properly wraps back from 4,294,967,295 to zero, but the receiving router that does not record the wrap event, causing the symptom to occur.

  Workaround: There is no workaround.

- CSCeb68925

  Symptoms: Enabling IP version 6 (IPv6) multicast routing by entering the **ipv6 multicast-routing** global configuration command may cause memory corruption. This situation may eventually cause the router to reload.

  Conditions: This symptom is observed on a Cisco 7200 series but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCeb69295

  Symptoms: A redistributed static route may not be advertised to any Border Gateway Protocol (BGP) peer, even though the route is selected as the best path in the BGP table.

  Conditions: This symptom is observed when the MPLS VPN Carrier Supporting Carrier IPv4 BGP Label Distribution feature is enabled and when the IP version 4 (IPv4) address family is missing from the running configuration.

  Workaround: There is no workaround.

- CSCeb77038

  Symptoms: A Cisco router may pause indefinitely because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0x60B5F1C0, address 0xEF4321E5
  ```

  Conditions: This symptom is observed on a Multiprotocol Label Switching (MPLS) provider edge (PE) router.

Workaround: There is no workaround.

- CSCeb85136

  Symptoms: An IP packet that is sent with an invalid IP checksum may not be dropped.

  Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped.

  Workaround: There is no workaround.

- CSCeb86563

  Symptoms: Multicast forwarding entries on a line card may become incorrect, causing packets to be forwarded to the Route Processor (RP). Packets may be dropped from the line card when the outgoing list becomes empty.

  Conditions: This symptom is observed after a high availability (HA) switchover has occurred.

  Workaround: Reload the line card after the HA switchover has occurred.

- CSCec06466

  Symptoms: A Cisco router may reload unexpectedly when the Designated Forwarder (DF) interface is changed to an interface that is already in the Outgoing Interface list (O-list).

  Conditions: This symptom is observed on a Cisco router that is configured for multicast Bidirectional PIM (Bidir-PIM).

  Workaround: There is no workaround.

- CSCec10494

  Symptoms: A Cisco router or switch may reload unexpectedly when you enter the **show ip igmp tracking detail** EXEC command.

  Conditions: This symptom is observed when the **ip igmp explicit-tracking** interface configuration command is enabled and the entries in the cache have expired.

  Workaround: There is no workaround.

- CSCec13278

  Symptoms: A Cisco router may generate continual tracebacks when you perform an online insertion and removal (OIR) of a line card.

  Conditions: This symptom is observed when Internet Group Management Protocol (IGMP) and IP Protocol Independent Multicast (PIM) are enabled.

  Workaround: Before you perform the OIR, disable IP PIM.

- CSCec15095

  Symptoms: A network link-state advertisement (LSA) may not be originated for an interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S, Release 12.2 S, Release 12.3, or Release 12.3 T when an interface that is configured for Open Shortest Path First (OSPF) and that is up has the same address as another interface that is shut down.

  Workaround: There is no workaround.

- CSCec16481

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml.

- CSCec24324

  Symptoms: A Cisco router may reload when you enter the **show ip hardware-cef** *prefix* command on a line card that uses hardware-based Cisco Express Forwarding (CEF) tables.

  Conditions: This symptom is observed on a Cisco 12000 series that is running Cisco IOS Release 12.0(26)S with Border Gateway Protocol (BGP) enabled.

  Workaround: There is no workaround.

- CSCec27239

  Symptoms: A Cisco router that processes external link-state advertisements (LSAs) may generate spurious memory access tracebacks or reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that runs Open Shortest Path First version 3 (OSPFv3).

  Workaround: There is no workaround.

- CSCec29868

  Symptoms: An Open Shortest Path First version 3 (OSPFv3) adjacency may flap when a standby Route Processor (RP) comes up after a switchover has occurred or after a router has reloaded. The router database may contain duplicate entries of the link link-state advertisement (LSA), or network LSA, or both.

  Conditions: This symptom is observed after a switchover has occurred when the interface number of the interface that is configured for OSPFv3 changes.

  This symptom is also observed after the router has reloaded when the interface number of the interface that is configured for OSPFv3 changes and when the neighbor still has the LSA (that was generated by the router on which the symptom occurs) with the old Link State ID (LSID) in its database. This situation may occur when the router does not clean up its LSA (for example, when the router reloads unexpectedly) or when the interface that connects to the neighbor is shut down before the router reloads and then brought back up after the router has reloaded.

  Workaround: There is no workaround.

- CSCec29953

  Symptoms: A retransmission counter may not be reset when a neighbor is terminated.

  Conditions: This symptom is observed on a Cisco platform that is running Open Shortest Path First (OSPF) when the retransmission limit default (12 or 24) is added to the retransmission mechanism.

  Workaround: Clear the OSPF process by entering the **clear ip ospf process** *pid* privileged EXEC command. Then, enter the **limit retransmissions non-dc disable** router configuration command.

- CSCec33377

  Symptoms: A router may experience a race condition that may cause the router to pause indefinitely when the router reloads.

  Conditions: This symptom is observed on a Cisco router under the following conditions:

  – A non-VPN routing/forwarding (VRF) Open Shortest Path First (OSPF) process is parsed.

  - A VRF OSPF process is parsed, but no router ID is available for the process.

  Workaround: There is no workaround.

- CSCec33773

  Symptoms: When a path is added to or deleted from the transit area between two virtual link routers that function as virtual link endpoints, the routes that are learned from the network backbone may not be updated in the routing table.

  Conditions: This symptom is observed when there are multiple equal-cost paths for virtual links in the transit area.

  Workaround: After the path in transit area has changed, enter the **clear ipv6 ospf force-spf** privileged EXEC command on the virtual link router that functions as a virtual link endpoint and that is not part of the network backbone.

- CSCec40377

  Symptoms: A multicast router may stop sending Protocol Independent Multicast (PIM) join messages.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(22)S, Release 12.0(22)SY, Release 12.1(13)E, or Release 12.2(14)S and that is configured for multicast routing when buffer allocation failures occur and when the I/O memory is low.

  Workaround: Disable and reenable multicast routing.

- CSCec40548

  Symptoms: A router may no longer be able to reach IP destinations through Open Shortest Path First (OSPF).

  Conditions: This symptom is observed when the **mpls traffic-eng area** *number* router configuration command is removed from the OSPF configuration.

  Workaround: Clear the OSPF process by entering the **clear ip ospf process** privileged EXEC and wait for the OSPF process to recover. This workaround is not recommended when there is a large routing table.

  Alternate Workaround: Reconfigure the **mpls traffic-eng area** *number* router configuration.

- CSCec43805

  Symptoms: The **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command may be missing from a Border Gateway Protocol (BGP) IPv4 Virtual Private Network (VPN) configuration in the output of the **show running-config** privileged EXEC command when all of the following keywords in the **address-family ipv4 vrf** *vrf-name* router configuration command are configured with their default values:

```
- aggregate-address    Configure BGP aggregate entries
- auto-summary         Enable automatic network number summarization
- bgp                  BGP specific commands
- default              Set a command to its defaults
- default-information  Control distribution of default information
- default-metric       Set metric of redistributed routes
- distance             Define an administrative distance
- distribute-list      Filter networks in routing updates
- exit-address-family  Exit from Address Family configuration mode
- help                 Description of the interactive help system
- maximum-paths        Forward packets over multiple paths
```

```
- neighbor              Specify a neighbor router
- network               Specify a network to announce via BGP
- no                    Negate a command or set its defaults
- redistribute          Redistribute information from another routing protocol
- synchronization       Perform IGP synchronization
- table-map             Map external entry attributes into routing table
```

However, the **distance bgp** *external-distance internal-distance local-distance* address family or router configuration command functions fine because the BGP administrative distance for the VPN in which the command is configured does get changed.

Conditions: The symptom is observed after the BGP IPv4 VPN configuration is saved in NVRAM and the router is reloaded.

Workaround: Change any of the keywords for the **address-family ipv4 vrf** *vrf-name* router configuration command (see the Symptoms section, above) to a nondefault value.

- CSCec44271

  Symptoms: The Multiprotocol BGP (MBGP) feature does not function when a router is configured as a Border Gateway Protocol (BGP) route reflector.

  Conditions: This symptom is observed when a BGP peer group has been enabled and then the MBGP feature is added.

  Workaround: Reset the BGP peer group by removing the peer group configuration and adding it back.

- CSCec45770

  Symptoms: A memory leak may occur on a router that runs IPv6 Open Shortest Path First version 3 (OSPFv3), and the following error message that is related to chunks may be generated:

  ```
  SYS-2-CHUNKSIBLINGS: Attempted to destroy chunk with siblings Tracebacks may also be
  generated.
  ```

  Conditions: This symptom is observed when a configuration change occurs in which prefixes are added or deleted or when the router reloads and the same prefix is advertised with a different Link State ID (LSID).

  Workaround: There is no workaround.

- CSCec48816

  Symptoms: When you remove **network** commands from a router, the router may reload unexpectedly with the following stacktrace:

  ```
  0x40AE7744:ospf_clean_if(0x40ae76c8)+0x7c
  0x40AE46FC:ospf_attach_interface(0x40ae4524)+0x1d8
  0x40AE20CC:ospf_parse_range(0x40ae1bb8)+0x514
  0x40AE1A7C:ospf_network_cmd_apply(0x40ae1a58)+0x24
  0x40AE1AC8:ospf_process_network_cmdQ(0x40ae1a88)+0x40
  0x40ADCC3C:ospf_router(0x40adca1c)+0x220
  ```

  Conditions: This symptom is observed on a Cisco router that has the **router ospf** global configuration command enabled and you remove **network** commands.

  Workaround: There is no workaround.

- CSCec51206

  Symptoms: A memory allocation failure (MALLOCFAIL) from the I/O memory pool may occur.

Conditions: This symptom is observed on a Cisco router that receives excessive multicast control traffic.

Workaround: Apply a quality of service (QoS) policy map to limit the rate of the multicast control traffic that can be received by the router.

- CSCec68467

  Symptoms: The memory usage of the Open Shortest Path First version 3 (OSPFv3) process may increase unexpectedly.

  Conditions: This symptom is observed on a Cisco router that runs OSPFv3 when OSPFv3 advertises routes and when you clear OSPFv3 by entering the **clear ipv6 ospf process** privileged EXEC command or when you configure or disable OSPFv3 by entering the **ipv6 router ospf** or **no ipv6 router ospf** router configuration command.

  Workaround: Shut down the interfaces on which OSPFv3 runs before you make changes to the OSPFv3 process by entering the commands stated in the Conditions, above.

- CSCec70664

  Symptoms: Routes on a provider edge (PE) router may take almost 10 minutes to propagate through a network because Border Gateway Protocol (BGP) remains in read-only mode for a long period of time.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that is a BGP peer to other PE routers. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb54512. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

- CSCec78690

  Symptoms: In rare situations, a User Datagram Protocol (UPD) Gigabit Route Processor (GRP) leader may bounce and cause problems when trying to converge other Border Gateway Protocol (BGP) peers.

  Conditions: This symptom occurs rarely on a Cisco GRP.

  Workaround: Enter the **clear ip bgp *** EXEC command to clear the symptom.

- CSCec81220

  Symptoms: Border Gateway Protocol (BGP) may reload when the outbound policy for a peer changes.

  Conditions: This symptom is observed on all Cisco platforms.

  Workaround: There is no workaround.

- CSCec82144

  Symptoms: A provider edge (PE) router may reload unexpectedly when you remove a loopback interface.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that is configured for Any Transport over MPLS (AToM) and Fast Reroute (FRR)

  Workaround: Do not remove the loopback interface when AToM and FRR are configured.

- CSCin51310

  Symptoms: You may not be able to configure the **ip vrf receive** interface configuration command.

  Conditions: This symptom is observed when the interface on which you attempt to configure the **ip vrf receive** interface configuration command does not have an IP address configured.

  Workaround: First configure an IP address on the interface, then enter the **ip vrf receive** interface configuration command on the interface.

- CSCin52817

  Symptoms: A Cisco router may reload unexpectedly when you manually reload the router.

  Conditions: This symptom is observed when the router is configured for Open Shortest Path First (OSPF).

  Workaround: There is no workaround.

ISO CLNS

- CSCec48833

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) routes that are learned from an IS-IS interface may not be added back to a Routing Information Base (RIB).

  Conditions: This symptom is observed on a Cisco router with an interface that is running IS-IS after you enter the **shutdown** interface configuration command followed quickly by the **no shutdown** interface configuration command.

  Workaround: Enable “ip routing protocol purge interface” on the router.

- CSCec61329

  Symptoms: It is not possible to configure an Intermediate System (IS)-type level-1 (L1) in an Intermediate System-to-Intermediate System (IS-IS) configuration on a Cisco router. The following error message is displayed:

  ```
  % Ambiguous command: "is-type level-1"
  ```

  Conditions: This symptom is observed on a Cisco 12000 series Internet router when attempts are made to set the IS type to L1. Level-1-2 (L1/2) and level-2 (L2) function correctly, and no error messages are displayed.

  Workaround: There is no workaround.

- CSCec73316

  Symptoms: The load-balancing ratio over Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels may not be the same ratio as the ratio that is configured on a Cisco router.

  Conditions: This symptom is observed because the Intermediate System-to-Intermediate System (IS-IS) method for checking the bandwidth change of an MPLS TE tunnel is different between Cisco IOS Release 12.0 S and Release 12.3 T.

  Workaround: There is no workaround.

- CSCec89671

  Symptoms: A router may reload when you enter the **no router isis** global configuration command.

Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7500 series when there is a large routing table and the **ip router isis** interface configuration command is configured on the router.

Workaround: Remove the **ip router isis** interface configuration command from the router, and then enter the **no router isis** global configuration command.

Miscellaneous

- CSCdu77394

  Symptoms: When a router initiates the FTP control and data connections, the source address for each connection is different.

  Conditions: This symptom does not exist if per-destination load balancing is used. Per-destination load balancing, however, causes some destinations to receive more traffic than others, which in turn causes some T1s to drop packets while others are hardly used. The **ip ftp source- interface** *interface* global configuration command affects only the control connection but not the data connection.

  Workaround: Enter the **no ip ftp passive** global configuration command or avoid having FTP servers initiate connections to the routers.

- CSCdz15807

  Symptoms: A file that is copied from a remote server to the running configuration file using secure file transfer (SCP) may fail with an error 26 (internal error).

  Conditions: This symptom is observed if the remote server is running the Linux operating system.

  Workaround: Use another file transfer method (for example, FTP).

- CSCdz18467

  Symptoms: Pings that have designated forwarder (DF) bits set and packet sizes greater than 1496 bytes are dropped.

  Conditions: This symptom is observed only on single-hop Multiprotocol Label Switching (MPLS) traffic-engineered (TE) tunnels.

  Workaround: There is no workaround.

- CSCdz30140

  Symptoms: When creating IP version 6 (IPv6) Access Control Lists (ACLs), the following message is displayed several times:

  ```
  %Access list already exists with these parameters
  ```

  In some cases, looking at the ACL indicates unwanted commands that are added, such as the following:

  ```
  permit ipv6 any any sequence 20
  deny 0 any any sequence 30
  ```

  These statements cannot be removed from the ACL. In other cases, lines of the ACL are modified. If a remark is added to the ACL once, then it will be repeated in ACL several times.

  Conditions: These symptoms are observed in Cisco IOS releases from Cisco IOS Release 12.0(23)S to Cisco IOS Release 12.0(26)S. The symptoms are seen only when the router has dual gigabit route processors (GRPs) installed and with different redundancy modes configured.

  Workaround: There is no workaround.

- CSCdz72292

  Symptoms: After a few weeks of normal operation, the interface on a Cisco PA- MC-8E1 begins flapping and finally pauses with the output queue stuck as follows:

```
Serial1/1:1 is up, line protocol is up
  Encapsulation HDLC, crc 16, Data non-inverted
  Keepalive set (120 sec)
  Last input 00:00:03, output 04:14:23, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 21952
  Queueing strategy: weighted fair
  Output queue: 30/4000/64/21855 (size/max total/threshold/drops)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     43903807 packets input, 3646461183 bytes, 0 no buffer
     Received 0 broadcasts, 321 runts, 0 giants, 0 throttles
     5160 input errors, 4 CRC, 0 frame, 0 overrun, 0 ignored, 2945 abort
     42026998 packets output, 2185017012 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     31 carrier transitions
  no alarm present
  Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags
```

  The following traceback is observed in the log:

```
%LINK-4-TOOBIG: Interface Serial60:1, Output packet size of 1526 bytes too big
Traceback= 0x604007F8 0x604A927C 0x6084E4D4 0x6057425C 0x60CE921C 0x60CE55EC
%LINK-4-TOOBIG: Interface Serial20:1, Output packet size of 1526 bytes too big
Traceback= 0x604007F8 0x604A927C 0x6084E4D4 0x6057425C 0x60CE921C 0x60CE55EC
```

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MC-8E1 interface.

  Workaround: There is no workaround.

- CSCdz80580

  Symptoms: A DPT-OC-12 port adapter (PA-SRP) may stop transmitting packets.

  Conditions: This symptom is observed on a Cisco uBR7200 series when a packet that is smaller than 8 bytes is transmitted on the PA-SRP.

  Workaround: Perform an online insertion and removal (OIR) of the PA-SRP.

- CSCdz83304

  Symptoms: A T3 link on a 4-port channelized OC-3 line card may not come up under Synchronous Digital Hierarchy (SDH) framing.

  Conditions: This symptom is observed on a Cisco 10000 series when the 4-port channelized OC-3 line card interoperates with third-party vendor test equipment.

  Workaround: Enter the **shutdown** controller configuration command followed by the **no shutdown** controller configuration command on the AU-3 controller that contains the T3 link.

- CSCea29102

  This caveat consists of two symptoms, two conditions, and two workarounds:

  1.

  Symptoms: A Route Processor (RP) may reload when you enter the **clear ip bgp *** privileged EXEC command while interfaces flap continuously.

  Conditions: This symptom is observed when Virtual Private Network (VPN) routing/forwarding (VRF) forwarding is configured on the interfaces that flap.

  Workaround: There is no workaround.

  2.

  Symptoms: An RP may reload when you simultaneously enter the **clear ip bgp *** privileged EXEC command and perform an online insertion and removal (OIR) by entering the **hw-reload reset** EXEC command.

  Conditions: This symptom is observed when you perform an OIR of an interface that has a VRF configuration in which the connected route is learned via a network statement. The connected route is removed when you perform the OIR.

  Workaround: Do not simultaneously enter the **clear ip bgp *** privileged EXEC command and perform an OIR.

- CSCea53696

  Symptoms: A FlexWAN module that is configured with a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7600 series when you apply Class-Based Weighted Fair Queueing (CBWFQ) on the PA-MC-STM-1 to a Multilink PPP (MLP) bundle that has E1 channels.

  Workaround: There is no workaround.

- CSCea62519

  Symptoms: Although traffic passes correctly when Frame Relay data-link connection identifier (DLCI) is configured, the output of the **show frame-relay pvc** privileged EXEC command does not display the input and output packets correctly.

  Conditions: This symptom is observed on a 1-port OC-12 Packet-over-SONET (POS) line card and a 6-port OC-3 POS line card that are installed in a Cisco 10000 series that is running Cisco IOS Release 12.0(24)S when Frame Relay DLCI is configured on the line cards.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.0(23)S.

- CSCea66218

  Symptoms: When a Tributary Unit Alarm Indication Signal (TU-AIS) is inserted for an E1 tributary on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) in an Synchronous Payload Envelope (SPE), packet corruption may occur on the adjacent E1.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7500 series.

  Workaround: There is no workaround.

- CSCea69601

  Symptoms: A flash Advanced Technology Attachment (ATA) disk card may become corrupted because of simultaneous accesses to the card. The corruption may not be immediately obvious. Signs of corruption are as follows:

  – You cannot use an image from the ATA disk card to boot up the router.

– Errors occur when data is stored on or read from the ATA disk card.

Conditions: This symptom is observed when you enter the **show file system** EXEC command while a file is being written to the ATA disk card or when you enter the **dir filesystem:** EXEC command while a file is being written to the same device as the target of the **dir filesystem:** EXEC command.

Workaround: Avoid using any commands that access the ATA disk card while a file is being written to the ATA disk card. If only the "disk0:" is used to store Cisco IOS images, it is not possible for the symptom to occur after copy completion. The integrity of the Cisco IOS image copied can be verified with the following two commands:

```
7500# fsck disk0:
Checking the partition table and boot sector...
Checking FAT, Files and Directories...
Reclaiming unused space...
Updating FAT...
fsck of disk0: complete

7500# verify disk0:rsp-pv-mz.120-26.S
%Filesystem does not support verify operations
Verifying file integrity
Verifying file disk0:rsp-pv-mz.120-26.S
[elided] ....Done!
Embedded Hash MD5 : 3F800F668A989A0BBC11B00EC4AB0551
Computed Hash MD5 : 3F800F668A989A0BBC11B00EC4AB0551
CCO Hash MD5 : 40A7E366287446157E8F0B3C76EE6F0B
Signature Verified
#
```

- CSCea76134

  Symptoms: External Border Gateway Protocol (eBGP) multipath load sharing may not use all of the available BGP paths.

  Conditions: This symptom is observed when all of the eBGP routes for the prefix that are affected are locally imported from another VPN routing/forwarding (VRF). As a result, a local label is not associated with the prefix in the imported VRF. This behavior prevents all BGP paths from being used.

  Workaround: Have at least one eBGP route for the prefix learned directly from an eBGP peer, instead of importing the route from another VRF. This forces the creation of a local label, and as a result, all BGP paths are used.

- CSCea84387

  Symptoms: A user session may pause indefinitely, causing a Cisco router to become unresponsive.

  Conditions: This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router via separate vty sessions.

  Workaround: Allow only one user at a time to enter MQC commands.

- CSCea87362

  Symptoms: Traffic may be blocked when Distributed Multilink Frame Relay (DMFR) is configured.

Conditions: This symptom is observed when the traffic is switched from the input interface by using fast switching rather than Cisco Express Forwarding (CEF).

Workaround: Configure CEF or distributed CEF (dCEF) on the input interface.

- CSCea88987

  Symptoms: A Cisco 10000 series does not support the 16-byte Path Trace Buffer (PTB) for Synchronous Digital Hierarchy (SDH) framing, which may cause difficulties for other platforms.

  Conditions: This symptom is observed on a Cisco 10000 series. The Cisco 10000 series does support a 64-byte PTB in which information is exchanged (IP address, chassis name, and so on).

  Workaround: There is no workaround.

- CSCeb01400

  Symptoms: At least 30 percent of the CPU of a Performance Routing Engine 1 (PRE-1) may be utilized to process flows, causing the number of packets that are processed per second to be much lower than you would expect.

  Conditions: This symptom is observed on a Cisco 10000 series when NetFlow and NetFlow export are enabled and when there is a large number of flows (more than 10,000).

  Workaround: Disable NetFlow.

  Alternate Workaround: Reduce the number of entries in the NetFlow cache of the Route Processor (RP) by entering the **ip flow-cache entries 1024** global configuration command. Doing so reduces the load of the CPU of the PRE-1. Note that the primary cache is located on the Parallel Express Forwarding (PXF) processor and supports a fixed number of 512 entries.

- CSCeb04441

  Symptoms: When an ATM link flaps or a remote ATM platform reloads, a Fast Etherchannel may fail and Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors that are connected via the Fast Etherchannel may be lost.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp-pv-mz image of Cisco IOS Release 12.0(21)S5.

  Workaround: There is no workaround.

- CSCeb16876

  Symptoms: A Cisco router may generate a “SYS-2-GETBUF” message during the “Tag Input” process and may reload unexpectedly.

  Conditions: This symptom is observed when the router fragments a Multiprotocol Label Switching (MPLS) packet.

  Workaround: There is no workaround.

- CSCeb18492

  Symptoms: When a new interface or subinterface is added, the following error message may appear on the console:

  ```
  ACLs could not add IDB to list
  ```

  If you have dual Route Processors (RPs), this message appears on the console of both RPs. This situation may lead to incorrect access control list (ACL) behavior when the ACL is modified or when a uCode reload occurs.

  Conditions: This symptom is observed on a Cisco 10000 series when a new interface that is configured with an access control list (ACL) is added after an old interface that was also configured with an ACL has been deleted. The symptom does not occur when the old interface that is deleted was not configured with an ACL.

Workaround: Remove the ACL configuration from the interface that you delete before you add a new interface.

- CSCeb21537

  Symptoms: When multicast is enabled, a Fast Ethernet (FE) egress interface may fail to function. Although the mroute table appears to be correct, packets are not forwarded from the FE interface.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeb23201

  Symptoms: An Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) may become stuck and not respond to changes in the state of its attachment circuit.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series or Cisco 7600 series that is configured for Ethernet over MPLS (EoMPLS) in VLAN mode.

  Workaround: There is no workaround.

- CSCeb27452

  Symptoms: A Cisco router that functions in a Multiprotocol Label Switching (MPLS) environment may reload unexpectedly with a bus error.

  Conditions: This symptom is observed under rare circumstances when the router attempts to send an Internet Control Message Protocol (ICMP) packet that was triggered by an MPLS packet.

  Workaround: There is no workaround.

- CSCeb34203

  Symptoms: A Cisco router may experience output queue packet drops on the priority queue before the interface is congested on an E1 serial interface on a PA-MC-E3.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.1(18)E. The symptom may also occur in other releases.

  Workaround: Enter the **tx-ring-limit** interface configuration command to increase the value of the drivers transmitted on the queue. see the following document for additional information:

  http://www.cisco.com/warp/customer/121/txringlimit_6142.html

- CSCeb35205

  Symptoms: A Cisco router may reload when a subdirectory is created on an Advanced Technology Attachment (ATA) Flash disk.

  Conditions: This symptom is observed when the ATA Flash disk space that is allocated to the subdirectory contains data from previously deleted files.

  When a subdirectory is created or extended, it is given space on the ATA Flash disk. If this space contains zeros, the symptom does not occur. However, if the space was previously used, the space does contain data bytes from the previous file, and these data bytes may confuse the file system. This situation may cause the router to reload.

  Workaround: Do not create subdirectories on the ATA Flash disk.

- CSCeb36929

  Symptoms: When a Cisco router is performing tag imposition, it may reload because of a bus error.

  Conditions: This symptom is observed when you create a new generic routing encapsulation (GRE) tunnel after the router has booted up and when GRE packets are received through this GRE tunnel and forwarded as Multiprotocol Label Switching (MPLS) packets.

Workaround: Enter the **tag-switching ip** interface configuration command followed by the **no tag-switching ip** interface configuration command on the newly-created GRE tunnel interface.

- CSCeb37367

  Symptoms: When the MPLS VPN Carrier Supporting Carrier feature is configured on a Cisco router, Label Distribution Protocol (LDP) may advertise a local label binding without installing an associated entry in the Multiprotocol Label Switching (MPLS) forwarding table. When peers of the Cisco router receive the advertised label binding and use the Cisco router as an MPLS next hop for the prefix for which there is no entry in the MPLS forwarding table, packet loss occurs.

  Conditions: This symptom is observed when the prefix is advertised by both Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP).

  Workaround: Deconfigure and then reconfigure BGP on the Cisco router.

  First Alternate Workaround: Reset the BGP connections.

  Second Alternate Workaround: Disable and then reenable IP over MPLS globally by using the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command.

- CSCeb44306

  Symptoms: A Cisco router that is configured with service policies may reload during the bootup process.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a Route Switch Processor 8 (RSP8) and a Versatile Interface Processor 4-80 (VIP4-80).

  Workaround: There is no workaround.

- CSCeb46191

  Symptoms: When a Cisco router is configured for both internal Border Gateway Protocol (iBGP) load balancing and Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN), incorrect MPLS labels may be installed. When one of the load-balancing links flaps, connectivity may be lost between the VPN sites.

  Conditions: This symptom is observed in the Cisco IOS releases that are listed in the “First Fixed-in Version” field at the following location:

  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdy76273.

  Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Disable iBGP load balancing.

- CSCeb47812

  Symptoms: A Cisco 7500 series or Cisco 7600 series may generate the following error message on its console:

  ```
  Invalid memory action (malloc) at interrupt level
  ```

  Conditions: This symptom is observed when you enter the **clear counters** EXEC command.

  Workaround: There is no workaround.

- CSCeb48648

  Symptoms: A Cisco 7500 series Frame Relay VC may not come up when configured as a cross-connect over an MPLS core.

  Conditions: This symptom is observed on a Cisco 7500 series that functions as a provider edge (PE) router and that provides a Frame Relay connection via an Any Transport over Multiprotocol Label Switching (AToM) tunnel over a core interface that is configured to use RSP-based Weighted Fair Queueing (WFQ).

  Workaround: Configure VIP-based queueing on the core-facing interface.

- CSCeb51428

  Symptoms: A Cisco router may reload unexpectedly after you have modified an access control list (ACL) and have entered the **clear pxf interface** privileged EXEC command.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not enter the **clear pxf interface** privileged EXEC command.

- CSCeb52270

  Symptoms: An interface of a Cisco router may not be able to receive traffic that is destined for an address that is configured on the router.

  Conditions: This symptom is platform independent and occurs only when there is a route in a different VPN routing and forwarding instance (VRF) that is attached or connected to the interface. This may occur when the route has been exported from one VRF to another or when a static route in a VRF points to the interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCeb52414

  Symptoms: When a Multiprotocol Label Switching (MPLS) traffic engineering (TE) headend receives a Resource Reservation Protocol (RSVP) path error message (with error code 25, “Notify”), the headend may tear down the label switched path (LSP) for the tunnel on which the path error message arrived, causing loss of packets on the affected tunnel.

  Conditions: This symptom is observed when the headend is a Cisco router that runs Cisco IOS Release 12.0(26)S or an earlier release and when some midpoint router generates a path error message (with error code 25, “Notify”) by using an error value other than 3. (An error value of 3 indicates that the tunnel is locally repaired.)

  Workaround: There is no workaround.

- CSCeb53323

  Symptoms: Packets may be forwarded to and switched on the Route Switch Processor (RSP) rather than on a Versatile Interface Processor (VIP).

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0 S when the Ethernet port on a VIP is configured for the Any Transport over MPLS (AToM): Ethernet over MPLS: Port Mode feature.

  Workaround: There is no workaround. The symptom occurs intermittently and normally can correct itself.

- CSCeb55043

  Symptoms: A secondary Route Switch Processor (RSP) may reload when a service policy is detached from an ATM permanent virtual circuit (PVC).

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with two RSPs in a redundant configuration.

  Workaround: First remove the PVC; then, recreate the PVC without the service policy attached to it.

- CSCeb56480

  Symptoms: A Label Distribution Protocol (LDP) session may not be established and may cause network connectivity problems (a ping may fail). The local LDP identifier is set to 0.0.0.0:0 instead of a valid identifier.

  Conditions: This symptom is observed in Multiprotocol Label Switching (MPLS) configurations when LDP is enabled.

  Workaround: Enter the **no mpls ip** router configuration command followed by the **mpls ip** router configuration command.

- CSCeb56909

  Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

  The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

  More details can be found in the security advisory which is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml.

- CSCeb56976

  Symptoms: Several Synchronous Digital Hierarchy (SDH) alarms and statistics do not function correctly for SDH channelizations when 1-channel OC-12 or 4-channel STM-1 line cards are used on a Cisco 10000 series router. These alarms and statistics are as follows:

  – The NEWPTR counter that is displayed in the output of the **show controllers sonet** EXEC command does not increment.

  – The Alarm Indication Signal (AIS) is asserted rather than the Loss of Multiframe (LOMF) as displayed in the output of the **show controllers au-4-tug-3** EXEC command.

  – The Binary Synchronous Communications (Bisync) IP (BIP)-2(TU-BIP) and Far End Block Error (FEBE) counters are not incremented or stored in the output of the **show controllers au-4-tug-3** EXEC command.

  – AIS is asserted under conditions in which Loss of Pointer (LOP) or Payload Label Mismatch (PLM) should be asserted.

  Conditions: These conditions are observed on a Cisco 10000 series that is running Cisco IOS Release 12.0 S or Release 12.2 BX.

  Workaround: There is no workaround.

- CSCeb57543

  Symptoms: A virtual circuit (VC) that controls tag switching may pause indefinitely.

  Conditions: This symptom is observed on a Cisco 7500 series when you repeatedly perform a manual redundancy switchover.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the affected VC is configured.

- CSCeb58316

  Symptoms: Multiprotocol Label Switching (MPLS) traffic engineering (TE) interarea and interautonomous system tunnels may fail to reoptimize.

  Conditions: This symptom is observed when a better path becomes available at a node or link beyond the area or interautonomous system of the tunnel headend.

  Workaround: There is no workaround.

- CSCeb59165

  Symptoms: A standby card may not be able to switch to the active state.

  Conditions: This symptom is observed in a Redundancy Framework (RF) environment when ATM, High-Level Data Link Control (HDLC), or Frame Relay clients synchronize data during the "standby-bulk" state.

  Workaround: There is no workaround.

- CSCeb61694

  Symptoms: A primary Performance Routing Engine 1 (PRE-1) may reload because of memory corruption.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of a 1-port Gigabit Ethernet line card.

  Workaround: There is no workaround. Note that the symptom does not occur with a 1-port Gigabit Ethernet half-height line card.

- CSCeb65079

  Symptoms: A Flash-disk timeout error such as the "ATA_Status time out waiting for 1" error may occur.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S and that is configured with an Advanced Technology Attachment (ATA) Flash disk.

  Workaround: To restore proper disk function, remove and reinsert the disk.

- CSCeb65671

  Symptoms: An incorrect virtual circuit (VC) disposition label may be generated, causing packets to drop.

  Conditions: This symptom is observed when VC label attributes, such as a control word setting or a VC type, do not match on a pseudowire.

  Workaround: Toggle the interface on which the pseudowire is configured by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCeb66010

  Symptoms: An interface may retain its Virtual Private Network (VPN) routing/forwarding (VRF) configuration when it should not.

  Conditions: This symptom is observed when you configure VRF forwarding on a loopback interface on a provider edge (PE) router, you delete the loopback, and then you add the loopback again.

  Workaround: Remove VRF forwarding from the loopback before you delete the loopback.

- CSCeb66997

  Symptoms: A Cisco 10720 may reload.

Conditions: This symptom is observed under rare circumstances when a SONET bit error rate (BER) is reported.

Workaround: There is no workaround.

- CSCeb67098

  Symptoms: A memory leak may occur in the Parallel Express Forwarding (PXF) interprocess communications (IPC) buffer on a Cisco 10720, as may be seen in the "toaster IPC buffer" counter in the output of the **show buffers** EXEC command.

  When the buffer pool is empty, the following error messages may appear, you may no longer be able to Telnet to the router, and the router may reload unexpectedly:

  ```
  %CAMR_QUEUE_CFG_GENERAL-3-EREVENT: Error @
  ../toaster/camr_rp/camr_tt_queue_cfg.c:463 -Traceback= 500DB204 500DB2BC 503954D8
  503986EC 50330A58

  %SYS-2-MALLOCFAIL: Memory allocation of 18196 bytes failed from 0x502C5BD0, alignment
  32 Pool: I/O Free: 552 Cause: Not enough free memory Alternate Pool: None Free: 0
  Cause: No Alternate pool

  -Process= "Pool Manager", ipl= 0, pid= 5 -Traceback= 50308EEC 5030A8E8 502C5BD8
  5031DD3C 5031DE7C
  ```

  Conditions: This symptom is observed on a Cisco 10720 when a policy map with a Weighted Random Early Detection (WRED) configuration that is enabled by using the **random-detect** policy-map class configuration command is applied to any interface of the router.

  The higher the rate with which the Route Processor (RP) sends packets to PXF, the faster the PXF IPC buffer leaks. However, the buffer may leak very slowly, and it may takes weeks before the buffer pool is empty.

  Workaround: Remove the policy maps with the WRED configuration from all interfaces of the router.

- CSCeb68830

  Symptoms: When an output policy map is applied to the interface of a 2-port OC-48 Spatial Reuse Protocol (SRP) uplink module or a 2-port OC-48 Packet-over-SONET (POS) uplink module, small packets (that is, IP packets with a size of 37, 38, or 39 bytes) that are sent out of the interface may be corrupted.

  Conditions: This symptom is observed on a Cisco 10720 that is configured with a policy-map configuration with a class map other than the class-default class map. The symptom does not occur when the policy-map configuration has the class-default class map.

  Workaround: Remove the policy-map configuration with the class map (other than the class-default class map) from the SRP or POS interface.

- CSCeb70856

  Symptoms: In an Inter-Autonomous System (InterAS), provider edge (PE) routers cannot ping each other. The next hop for PE interfaces is not the loopback address of the Autonomous System Boundary Router (ASBR) within the same AS because the **neighbor next-hop self** router configuration command does not function in Border Gateway Protocol (BGP).

  Conditions: This symptom is observed on a Cisco 10720 ASBR in an InterAS with a 6PE router that has a route reflector (RR).

  Workaround: There is no workaround.

- CSCeb70879

  Symptoms: IP version 4 (IPv4) fragments may be corrupted in the following way: The first 8 bytes of a fragment duplicate the last 8 bytes of the previous fragment.

Conditions: This symptom is observed on a Cisco 10720 that runs Cisco IOS Release 12.0(24)S or a later release when you send IPv4 traffic from a Fast Ethernet (FE) ingress interface to an FE egress interface.

Workaround: There is no workaround.

- CSCeb71938

  Symptoms: In a redundancy configuration, a secondary Performance Routing Engine (PRE) may continue to reload at startup and not complete its bootup process.

  Conditions: This symptom is observed on a Cisco 10000 series when the **switchover timeout** *timeout-period* redundancy configuration (main-cpu mode) command is configured, when you have entered **0** for the *timeout-period* argument, and when the secondary PRE is reset.

  To recover form the symptom, power cycle the router, or perform the following steps:

  1. Remove the affected secondary PRE.

  2. Reload the primary PRE.

  3. When the Primary PRE has booted, deconfigure the **switchover timeout** *timeout-period* redundancy configuration (main-cpu mode) command.

  4. Reinstall the secondary PRE, which should bootup normally.

  Workaround: Do not configure the **switchover timeout 0** redundancy configuration (main-cpu mode) command. Note that the symptom occurs only when you have entered **0** for the *timeout-period* argument, not when you have entered other values.

- CSCeb72516

  Symptoms: The **neighbor** *ip-address* **send-label** address family configuration command may not function properly for an IP version 6 (IPv6) Border Gateway Control (BGP) neighbor that is part of a BGP peer group in an IPv6 address family; the functionality of the **send-label** keyword may not be advertised to the peers.

  Conditions: This symptom is observed when you use BGP peer groups with a provider edge (PE) router that is running IPv6 in a Multiprotocol Label Switching (MPLS) environment (referred to as a 6PE router).

  Workaround: Enter the **neighbor** *ip-address* **send-label** address family configuration command for the IPv6 BGP neighbor before you make the IPv6 BGP neighbor part of the BGP peer group in the IPv6 address family.

- CSCeb73758

  Symptoms: When you configure a Cisco 10000 series, messages similar to the following ones may appear, and a VLAN may not be enabled:

  ```
  %GENERAL-3-EREVENT: c10k_dot1q_vlan_enable: No tt_info
  -Traceback= 60142770 60142A50 603AEC40 603AE06C 603ADCE0 6036EAD8 60193BA8 60380DD4
  60B85BEC 60B861D4 603D6FAC 603D6F98
  %GENERAL-3-EREVENT: get_injection_vcci: no info for VLAN ID 972
  -Traceback= 600DF180 6009AF2C 6009B178 603A831C 604BB804 605013F0 605018A8 605014E0
  602B8D84 602B94A4 604F2DC0 604F33F4 60504DB4 60504BA4 60504984 6052351C
  %GENERAL-3-EREVENT: get_injection_vcci: no info for VLAN ID 972
  -Traceback= 600DF180 6009AF2C 6009B178 603A831C 604BB804 605013F0 605018A8 60504E0
  602B8D84 602B94A4 604F2DC0 604F33F4 60504DB4 60504BA4 60504984 6052351C
  ```

  Conditions: This symptom is observed on a Cisco 10000 series when you change the encapsulation of a LAN subinterface to dot1q encapsulation while the subinterface is shut down.

When the symptom occurs, the output of the **show hardware pxf cpu subblocks** privileged EXEC command lists “noSB” for the affected subinterface, as is indicated in the following example:

```
Router# show hard pxf cpu sub | i GigabitEthernet4
GigabitEthernet4/0/0 up 12000 4 PXF 1 81C4A800 4
GigabitEthernet4/0/0.500 administ 12000 4 PXF 1 81C4A800 noSB
```

Workaround: Change the encapsulation of the subinterface to dot1q when the subinterface is not shut down. The state of the main interface is irrelevant. After you change the encapsulation, you can shut down the subinterface again.

When the subinterface is created while the main interface is shut down, the subinterface and the VLAN do not function properly. Perform the following steps to recover the VLAN:

1. Ensure that the subinterface is not shut down.
2. (Optional) Enter the **no encapsulation dot1q native** subinterface configuration command.
3. Remove the subinterface.
4. Recreate the subinterface.
5. Change the encapsulation back to dot1q.

- CSCeb76341

  Symptoms: A label may not be assigned for a peer provider edge (PE) router.

  Conditions: This symptom is observed on a Cisco 7500 series and a Cisco 12000 series in a Virtual Private Network (VPN) configuration with multiple route reflectors (RRs) and label controlled ATM (LC-ATM) links between PE routers. The symptom may also occur on other platforms.

  Workaround: There is no workaround.

- CSCeb76642

  Symptoms: A Cisco router may reload when you enter the **show ip cef non-recursive detail** EXEC command.

  Conditions: This symptom is observed when any **show** command attempts to display information about tag rewrite entries while the tag rewrite entries are being deleted by route updates.

  Workaround: Do not enter any **show** command to display tag rewrite entries when many route updates occur.

- CSCeb77493

  Symptoms: When Layer 2 Tunneling Protocol version 3 (L2TPv3) is configured, a significant degradation in performance may occur.

  Conditions: This symptom is observed on a Cisco 7200 series and Cisco 7500 series that run Cisco IOS Release 12.0 S.

  Workaround: There is no workaround.

- CSCeb78329

  Symptoms: After a Route Processor Redundancy Plus (RPR+) switchover occurs, the deletion of an existing permanent virtual circuit (PVC)/permanent virtual path (PVP) fails. This situation prevents you from recreating the same PVC/PVP. You can create a new PVC/PVP, but once you delete it, you cannot recreate it because the PVC remains in the active state.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.0 S or Release 12.0 SX.

  Workaround: There is no workaround. To enable the router to return to normal operation, reload the router.

- CSCeb78610

  Symptoms: The interface protocol may not come up for a 1-port OC-12 Packet-over-SONET (POS) line card when the **encapsulation frame-relay** interface configuration command is configured.

  Conditions: This symptom is observed on a Cisco 10000 series when the 1-port OC-12 POS line card is connected back-to-back to another line card in another Cisco 10000 series.

  Workaround: There is no workaround.

- CSCeb79576

  Symptoms: An outgoing label may not be installed in the Label Forwarding Information Base (LFIB) for an IP version 4 (IPv4) prefix.

  Conditions: This symptom is observed when the prefix is learned via a Border Gateway Protocol (BGP) session. This situation may occur when the prefix is deleted in the Label Information Base (LIB) and not allocated to any local label binding.

  Workaround: There is no workaround.

- CSCeb79911

  Symptoms: Backward explicit congestion notification (BECN) packets may be dropped by an Any Transport over Multiprotocol Label Switching (AToM) tunnel.

  Conditions: This symptom is observed when you configure AToM in the network core, the network core contains Frame Relay interfaces, and BECN is enabled.

  Workaround: There is no workaround.

- CSCeb80481

  Symptoms: A memory leak may occur in the "SNMP Engine" process, which can be verified in the output of the **show processes memory | SNMP ENGINE** privileged EXEC command.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(26)S and Release 12.2(18)S when you enter the **snmpget** command for the MPLS-LSR-MIB MIB.

  Workaround: There is no workaround.

- CSCeb80992

  Symptoms: A Catalyst 6000 series Supervisor 2 may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when access control list (ACL) counters are sent from a line card to the Route Processor (RP) and when the ACL number is in the expanded range (that is, from 1300 to 1999 or from 2000 to 2699).

  Workaround: There is no workaround.

- CSCeb82737

  Symptoms: When you shut down the last port of an 8-port Fast Ethernet half-height line card (port 7), all other ports on the line card may stop transmitting traffic.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not shut down port 7. If port 7 is shut down, enter the **no shutdown** interface configuration command on the interface to enable traffic to resume on the other interfaces.

- CSCeb86270

  Symptoms: In Cisco IOS software that is running Multiprotocol Label Switching (MPLS), the Label Distribution Protocol (LDP) peer address table may become corrupted and cause the router to reload.

Conditions: This symptom may be observed in situations where three or more routers have advertised the same IP address in LDP address messages. This normally happens when routers have been misconfigured but in very rare circumstances may be done deliberately.

The circumstance can be recognized by the presence of the following error message:

```
%TAGCON-3-DUP_ADDR_RCVD: Duplicate Address 10.0.0.1 advertised by peer 10.2.2.2:0 is
already bound to 10.1.1.1:0
```

If only one such message is seen for a given IP address (10.0.0.1 in the above example) then only two routers have advertised the IP address, and only the second is being treated as a duplicate. At least one more such message should be seen if at least three routers have advertised the IP address in question.

Workaround: The symptom does not occur in typical configurations because duplicate addresses are not configured. If such a configuration is accidentally done, the failure may be avoided if the configuration is corrected before the LDP session to any of the involved peers goes down. If the configuration is deliberate, there is no workaround.

- CSCeb87159

  Symptoms: The CNS event agent does not detect when the connection to the server breaks.

  Conditions: This symptom is observed when the CNS event agent service is configured by the **cns event keepalive** configuration command.

  Workaround: There is no workaround.

- CSCeb87444

  Symptoms: IP packets may be dropped from an input EtherChannel interface when Cisco Discovery Protocol (CDP) is enabled.

  Conditions: This symptom is observed on a Cisco 10720 when EtherChannel and CDP are enabled on every interface in the router.

  Workaround: Disable CDP on the interfaces that are part of the EtherChannel channel group.

- CSCec00268

  Symptoms: A multilink interface may stop processing received packets.

  Conditions: This symptom is observed on a Cisco 7500 series when Multilink PPP (MLP) is configured and when a lot of traffic is forwarded to the process-switching path.

  Workaround: To clear the symptom, move the physical interfaces to a new multilink interface with a new interface number.

- CSCec00370

  Symptoms: An Internet Control Message Protocol version 6 (ICMPv6) checksum error may be generated, causing a ping to fail.

  Conditions: This symptom is observed on a Cisco 10720 when an IP version 6 (IPv6) ping of 291 bytes or more is performed on a Gigabit Ethernet interface, or when an IPv6 ping of 305 bytes or more is performed on a Fast Ethernet interface.

  Workaround: There is no workaround.

- CSCec02911

  Symptoms: Normal priority IP packets do not exit the queue fast enough on a Cisco router during a heavy load period. The router is unmanageable, and pings and Telnet sessions fail. All PPP over ATM (PPPoA) and Layer 2 Tunneling Protocol (L2TP) tunnels are lost. This symptom may be observed by reviewing the output of the **show ip spd** EXEC command.

Conditions: These symptoms are observed on a Cisco 10000 series router that has a heavy load (10,000 PPP over Ethernet [PPPoE] PPP terminated aggregation [PTA] sessions with 6000 PPPoA sessions and 6000 active L2TP tunnels). Under these load conditions, when the 10,000 PTA sessions are cleared, the router stays at 100 percent CPU utilization for approximately 10 minutes.

Workaround: There is no workaround.

- CSCec02935

  Symptoms: A Cisco router that has Parallel Express Forwarding (PXF) enabled does not function after it reloads.

  Conditions: This symptom is observed on a Cisco 10720 that has PXF enabled and that applies the weighted random early detection (WRED) configuration to multiple interfaces.

  Workaround: Remove the WRED configuration on the interfaces.

- CSCec03392

  Symptoms: Tracebacks may be observed when a 6-port OC-3 Packet over SONET (POS) line card is configured with the **encapsulation frame-relay** interface configuration command.

  Conditions: This symptom is observed on a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCec03782

  Symptoms: A memory allocation failure may occur on compiled access control list (ACL) tables. There may be continued attempts to recompile the ACLs that fail.

  Conditions: This symptom is observed when compiled ACLs are enabled by entering the **access-list compiled** global configuration command, and the total number of ACL entries is relatively large (over 1500 lines). Random or constantly changing traffic patterns may cause the compiled ACL tables to grow to the point at which memory fragmentation causes the memory allocation failure.

  Workaround: Disable and then reenable the compiled ACLs by entering the **no access-list compiled** global configuration command followed by the **access-list compiled** global configuration command.

  Alternate Workaround: Completely disable the compiled ACLs.

  Second Alternate Workaround: ACLs may sometimes be rearranged to make the list shorter or less complex. This will reduce the memory requirements. Large ACLs used for Border Gateway Protocol (BGP) route prefixes may be converted to use a prefix list configuration instead.

- CSCec03896

  Symptoms: Large packets may not be fragmented when both Frame Relay fragmentation (FRF.12) and a service policy are enabled on a channelized interface.

  Conditions: This symptom is observed when the service policy is an output service policy that is configured for Class-Based Weighted Fair Queueing (CBWFQ)/Low Latency Queueing (LLQ) or fair queueing.

  Workaround: There is no workaround. (Removing the service policy is not an acceptable workaround.)

- CSCec03907

  Symptoms: A Route Switch Processor 4 Plus (RSP4+) may reload.

  Conditions: This symptom is observed on a Cisco 7500 series when you configure the **interface loopback** *interface-number* interface configuration command on an interface of the router and the value of the *interface-number* argument is a 9-digit number that starts with 10.

  Workaround: If possible, use another range of numbers for the numbers that are assigned to the loopback interfaces, that is, a range of numbers that do not start with 10.

- CSCec04473

  Symptoms: A Versatile Interface Processor (VIP) may reload when you remove a service policy from a Frame Relay (FR) permanent virtual circuit (PVC).

  Conditions: This symptom is observed on a Cisco 7500 series during a high traffic load.

  Workaround: Shut down the interface or subinterface on which the FR PVC is configured before you remove the service policy.

- CSCec06146

  Symptoms: A serial interface of a 1-port multichannel E3 port adapter (PA-MC-E3) may fail to enter the "up/up" state when you initially configure the interface or after a number of reconfigurations.

  Conditions: This symptom is observed on a PA-MC-E3 that is installed in a Cisco 7500 series or Cisco 7600 series when the following sequence of events occurs:

  1. You configure an interface by entering the **controller e3** *slot/port* global configuration command followed by the **e1** *line-number* **channel-group** *channel* **timeslots** *range* controller configuration command.
  2. You delete the interface by entering the **controller e3** *slot/port* global configuration command followed by the **no e1** *line-number* **channel-group** *channel* controller configuration command.
  3. You reconfigure the interface by entering the commands listed in Step 1.

  Although the symptom may occur when you initially configure the interface, it is more likely to occur when you configure, delete, and reconfigure the interface several times.

  Workaround: When the interface does not enter the "up/up" state, configure the interface again.

- CSCec06275

  Symptoms: The following error message may be displayed on the console of a Route Switch Processor (RSP):

  ```
  %CBUS-3-CMDDROPPED: Cmd dropped,CCB 0xF800FFB0,slot 9, cmd code 24
  ```

  Conditions: This symptom is observed on a Cisco 7500 series when software compression is enabled on serial interfaces and dialer interfaces and when Cisco Express Forwarding (CEF) switching rather than distributed CEF (dCEF) switching is enabled. This situation causes software compression to occur on the RSP.

  Because software compression is enabled on all the serial interfaces, the CPU utilization of the RSP becomes very high, causing commands to be dropped.

  Workaround: Remove software compression from the serial interfaces.

- CSCec07487

  Symptoms: An interface may not transmit traffic because the output may be stuck. When this symptom occurs, the console of the Route Switch Processor 4 (RSP4) may display the following error messages:

  ```
  %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se1/0/2:15, TEI0 changed to down
  ```

```
%ISDN-6-LAYER2DOWN: Layer 2 for Interface Se1/0/1:15, TEI0 changed to down
%ISDN-6-LAYER2DOWN: Layer 2 for Interface Se1/0/3:15, TEI0 changed to down
%RSP-3-RESTART: interface Serial1/0/0:15, not transmitting
Output Stuck on Serial1/0/0:15
%RSP-3-RESTART: interface Serial1/0/1:15, output frozen
%RSP-3-RESTART: interface Serial1/0/2:15, not transmitting
%RSP-3-RESTART: cbus complex
```

Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.1(19)E1 when the **compress stac caim** interface configuration command is configured on the interface. The symptom may also occur in other releases.

Workaround: Remove the **compress stac caim** interface configuration command from the interface.

- CSCec09193

  Symptoms: When a subinterface is configured with a subinterface number value larger than 65535, the protocol enabled on this subinterface may not be in the proper state for correct operation after the switchover.

  Conditions: These symptoms have been observed on Cisco platforms with redundant Route Processors operating in stateful switchover (SSO) redundancy mode.

  Workaround: Limit the subinterface number value to an integer less than 65535 while configuring subinterfaces.

- CSCec12741

  Symptoms: If an access control list (ACL) is recompiled under heavy load conditions, CPUHOG messages may be generated.

  Conditions: This symptom is observed when compiled ACLs are enabled by entering the **access-list compiled** global configuration command, and the total number of ACL entries is relatively large (over 1500 lines). Random or constantly changing traffic patterns may cause the CPUHOG messages. A side effect of this symptom is that not enough time is provided for other processes, and areas such as keepalives or Cisco Express Forwarding (CEF) management may be impacted.

  Workaround: Disable and then reenable the compiled ACLs by entering the **no access-list compiled** global configuration command followed by the access-list compiled global configuration command.

  Alternate Workaround: Disable the compiled ACLs completely.

- CSCec14259

  Symptoms: Multicast packets are not correctly classified by input Quality of Service (QOS) which causes police, set, and other QoS actions to fail on the multicast packets.

  Conditions: These symptoms are observed when QoS is configured on an interface.

  Workaround: There is no workaround.

- CSCec15723

  Symptoms: A router reloads unexpectedly because of a bus error, which causes a failover to the redundant PRE.

  Conditions: These symptoms have been observed on a Cisco router that is running Cisco IOS Release 12.0(25)S1.

  Workaround: There is no workaround at the current time.

- CSCec15733

  Symptoms: A Cisco router that is running IP over Multiprotocol Label Switching (MPLS) may reload when the Label Distribution Protocol (LDP) responds to the creation of a new session.

  Conditions: This symptom is observed when the router is operating under extremely stressful conditions that cause the CPU utilization to be close to 100 percent. This situation rarely occurs.

  Workaround: There is no workaround.

- CSCec16666

  Symptoms: Two channel group interfaces on a 1-port multichannel STM-1 port adapter (PA-MC-STM-1) may receive the same ifIndex. This can be observed in the following command output:

  ```
  show snmp mib ifmib ifindex serial X/X/X:0
  Interface = SerialX/X/X:0, Ifindex = 496
  show snmp mib ifmib ifindex serial Y/Y/Y:0
  Interface = SerialY/Y/Y:0, Ifindex = 496
  ```

  Conditions: This symptom is observed when some of the E1 interfaces are deleted and recreated.

  Workaround: Do not delete any of the E1 interfaces.

- CSCec17262

  Symptoms: In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN), if a router receives an MPLS packet with an IP version 4 (IPv4) option underneath, and the MPLS packets have two or more labels, when the router tries to untag all labels, Parallel Express Forwarding (PXF) stops.

  Conditions: This symptom is observed on a Cisco 10720 router that acts as an MPLS VPN provider edge (PE) router.

  Workaround: There is no workaround. The symptom has not been observed in a basic MPLS network without VPN (this means there is only one label).

- CSCec18181

  Symptoms: A Cisco 7200 series may reload when you enter the **show pas i82543 interface gigabitEthernet** *number* **mta** privileged EXEC command.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a Network Processing Engine G-1 (NPE-G1).

  Workaround: There is no workaround.

- CSCec21012

  Symptoms: After a manual switchover is performed on a dual Route Processor (RP) router that is in Stateful Switchover (SSO) mode, a secondary RP may reload.

  Conditions: This symptom is observed on a Cisco 12000 series router with an 8x OC3 ATM line card that is running the gsr-p-mz image of Cisco IOS Release 12.0(26.1)S.

  Workaround: There is no workaround.

- CSCec21999

  Symptoms: A port on an OC-3 ATM line card may display an LCD alarm when the router reloads. This alarm may bring down the controller and interface. The far end functions properly but is unable to pass traffic because of the downed interface.

Conditions: These symptoms are observed only when the router reloads but the symptoms do not occur with every reload.

Workaround: Perform the following steps: 1. Put the port into diagnostic serial loopback. 2. Remove the diagnostic serial loopback.

For example:

```
conf t
int atm7/0/0
loopback diagnostic serial
end

conf t
int atm7/0/0
no loopback diagnostic serial
end
```

- CSCec22252

  Symptoms: A Cisco 7500 series may reload when one of the physical multilink member interfaces is shut down while traffic passes through the interface of the multilink member.

  Conditions: This symptom is observed on a Cisco 7500 series and is specific to configuring tag switching (and not VPN routing/forwarding [VRF] forwarding) on a multilink interface that is based on Versatile Interface Processor (VIP) channels or serial interfaces in the distributed mode (for example, the symptom may occur only if a P-provider edge [PE] link is implemented over the multilink interface).

  Workaround: Shut down the Multilink PPP (MLP) interface first, and then shut down the MLP physical subinterface as needed.

- CSCec24986

  Symptoms: Parallel Express Forwarding (PXF) stops and then reloads if you issue a ping immediately after a policy map attaches to an interface.

  Conditions: This symptom is observed if you apply quality of service (QoS) policy maps on the input Gigabit Ethernet (GE) line card, and output ATM interface of a Multiprotocol Label Switching (MPLS) provider edge (PE) router.

  Workaround: Delay a few seconds after you attach the policy map to the interface before you issue the ping.

- CSCec25317

  Symptoms: A Versatile Interface Processor 4 (VIP4) in which an 8-port multichannel E1, G.703 120 ohm interface port adapter (PA-MC-8E1/120) is installed may reload unexpectedly and display the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address.
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that has a distributed multilink interface on which IP Header Compression (IPHC) is configured when distributed Cisco Express Forwarding (dCEF) is disabled by entering the **no ip cef distributed**) global configuration command and reconfigured by entering the **ip cef distributed** global configuration command while the interface is operational.

  Workaround: Ensure that the multilink interface is shut down before you to disable dCEF.

- CSCec26076

  Symptoms: When you enter the **interface** *type* **1/0.0** global configuration command to configure subinterface 0, the command does not configure the subinterface but the main interface; that is, the command is executed as if you had entered the **interface** *type* **1/0** global configuration command.

  Conditions: This symptom is observed when you configure an ATM, Fast Ethernet, or Gigabit Ethernet subinterface; that is you enter **atm**, **fastethernet**, or **gigabitethernet** for the *type* argument.

  Workaround: There is no workaround. You cannot configure subinterface 0. The fix for this caveat changes the subinterface range from the 0-to-4294967295 range to the 1-to-4294967295 range.

- CSCec26539

  Symptoms: A Cisco router that has a Hot Standby Router Protocol (HSRP) group configured on a subinterface may stop responding and may reload.

  Conditions: This symptom is observed when an HSRP Simple Network Management Protocol (SNMP) query is performed. The symptom occurs only when HSRP is configured on a subinterface. The symptom does not occur for an HSRP group that is configured on a major interface.

  Workaround: Do not initiate an SNMP query for HSRP.

  Alternate Workaround: Use the **snmp-server** global configuration commands to specify which MIBs are available (for example):

  snmp-server view HSRP internet included

  snmp-server view HSRP ciscoHsrpMIB excluded

  snmp-server view HSRP ciscoHsrpExtMIB excluded

  snmp-server community public view HSRP RW 20

  snmp-server community private view HSRP RW 20

- CSCec26563

  Symptoms: A Cisco router that is in the process of setting up a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed under unusual circumstances when the following series of events occur:

  – You disable MPLS TE tunnels on the router by entering the **no mpls traffic-eng tunnels** global configuration command.

  – You enter one of the following MPLS TE interface configuration commands on an interface:

    mpls traffic-eng attribute-flags *attributes*

    mpls traffic-eng administrative-weight *weight*

    mpls traffic-eng flooding thresholds

  – The router attempts to set up a TE tunnel over this interface while the interface state changes to "up." (This event causes the router to reload.)

  Workaround: Before you enter any of the above-mentioned MPLS TE interface configuration commands on the interface, ensure that MPLS TE tunnels are enabled on the interface by entering the **mpls traffic-eng tunnels** interface configuration command. Before you disable MPLS TE tunnels on the interface by entering the **no mpls traffic-eng tunnels** interface configuration command, ensure that any of the above-mentioned MPLS TE interface configuration commands are removed from the interface.

- CSCec26773

  Symptoms: A router may reload when there is an active intercept and a Performance Routing Engine (PRE) cutover occurs.

  Conditions: This symptom is observed on a Cisco 10000 series that is running the c10k-u2p10-mz image of Cisco IOS Release 12.0(25)S1.

  Workaround: There is no workaround.

- CSCec27278

  Symptoms: On a Cisco router that is configured with a Multilink PPP (MLP) interface, the available processor memory may decrease rapidly because of a memory leak.

  Conditions: This symptom is observed when the MLP interface flaps repeatedly.

  Workaround: There is no workaround. You must resolve the cause of the flapping MPL interface.

- CSCec28540

  Symptoms: A Cisco 7200VXR router generates a traceback that points to memory depletion after the Cisco IOS software loads on the router.

  Conditions: This symptom is observed on a Cisco 7200VXR that is configured with Multiprotocol internal Border Gateway Protocol (MP-iBGP) to create Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) sessions. After a few minutes, tracebacks are generated and I/O memory is depleted.

  Workaround: There is no workaround.

- CSCec30795

  Symptoms: If traffic passes on multiple ports of an 8-port Fast Ethernet (FE) card and the **shutdown** interface configuration command is entered on one of the traffic-flowing ports, all the other ports stop passing traffic.

  Conditions: This symptom is observed on a Cisco 10000 series with an 8-port Fast Ethernet (FE) card that is running a Performance Routing Engine 1 (PRE1) image of Cisco IOS Release 12.0(23)S4. There is no special configuration required to experience this symptom. Ports that pass traffic with a basic default configuration will experience the symptom.

  Workaround: Enter the **no shutdown** interface configuration command to free the other ports. Do not shut down any port on an 8-port Half Height (HH) FE line card until a fix is available.

- CSCec30960

  Symptoms: A Cisco router may reload when deconfiguration and configuration files are copied to the router for a 1-port OC12 ATM line card.

  Conditions: This symptom is observed on a Cisco 10000 series router when Automatic Protection Switching (APS) is configured for the 1-port OC12 ATM line card.

  Workaround: There is no workaround.

- CSCec31110

  Symptoms: The output from the **show interfaces gige stats** EXEC command may incorrectly display a large value.

  Conditions: This symptom is observed on a Gigabit Ethernet (GE) interface in a PPP over Ethernet (PPPoE) environment.

  Workaround: There is no workaround.

- CSCec31162

  Symptoms: Incorrect tags may be imposed after a route has flapped.

  Conditions: This symptom is observed on a Cisco router that functions in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment.

  Workaround: There is no workaround.

- CSCec31512

  Symptoms: When you enter the **send break** command on the active CPU and keep the active CPU in the ROM monitor (ROMmon) mode for a long time, the standby CPU may reload because of a bus error exception.

  Conditions: This symptom is observed on a Cisco ONS 15540.

  Workaround: There is no workaround.

- CSCec31781

  Symptoms: After the **redundancy force-switchover** privileged EXEC command is entered on a Cisco router, a Versatile Interface Processor (VIP) may reload when the router returns to the Stateful Switchover (SSO) mode.

  Conditions: This symptom is observed on a Cisco 7500 series that is running the rsp-pv-mz image of Cisco IOS Release 12.0(25)S1.

  Workaround: There is no workaround.

- CSCec31790

  Symptoms: The following error may cause a Cisco 10000 series to reload:

  ```
  %ERR-1-GT64120 (PCI-0): Fatal error, Memory parity error (external)
  ```

  Conditions: This symptom is observed on a Cisco 10000 series when a single bit Error-Correcting Code (ECC) error is detected in the Synchronous Dynamic RAM (SDRAM).

  Workaround: There is no workaround.

- CSCec34475

  Symptoms: When you load the Cisco IOS field diagnostic software image from a Flash card, the router reloads.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(16)BX or Release 12.2(16)BX1.

  Workaround: Load the field diagnostic image from TFTP or from bootflash.

- CSCec35827

  Symptoms: A line card may reload when the priority configuration is removed from a service policy.

  Conditions: This symptom is observed on the serial interface of a Cisco router that has Frame Relay encapsulation configured.

  Workaround: There is no workaround.

- CSCec37097

  Symptoms: Fast Reroute (FRR) fails to detect a protected interface that has gone down. Initial failure detection varies from 100 to 800 milliseconds.

  Conditions: This symptom is observed only on a Cisco 7500 series router.

  Workaround: There is no workaround.

Further Problem Description: When the protected interface goes down, FRR switches from the primary tunnel to the backup tunnel.

- CSCec37930

  Symptoms: The standby Route Switch Processor (RSP) for a Cisco 7500 series may reload unexpectedly.

  Conditions: This symptom is observed on an RSP for a Cisco 7500 series that has a LAN Extender (LEX) interface configured, and that has the Stateful Switchover (SSO) feature enabled.

  Workaround: There is no workaround.

- CSCec38322

  Symptoms: A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) provider edge (PE) router that is running distributed Cisco Express Forwarding (dCEF) may have high memory usage and memory allocation failures when dCEF is disabled and then reenabled.

  Conditions: This symptom is observed on a PE router that has a large number of VPN routes (over 30,000) in a VPN routing/forwarding (VRF) table when CEF is disabled and then reenabled.

  Further Problem Description: View the output of the **show processes memory** EXEC command to verify that the CEF process memory usage increases.

  Workaround: Reload the router.

- CSCec41955

  Symptoms: The ATM over Multiprotocol Label Switching (MPLS) port mode connection may stay in the down state after the cell-packing timer index is modified.

  Conditions: This symptom is observed on a provider edge (PE) router with the packed cell relay feature enabled.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the port to bring back the connection.

- CSCec42855

  Symptoms: The following symptoms are observed on a dual Route Switch Processor 8 (RSP8) router with a CT3 interface:

  1. When the router runs Cisco IOS Release 12.0(23)S4 everything functions correctly. After the router is upgraded to Cisco IOS Release 12.0(26)S, distributed Cisco Express Forwarding (dCEF) does not run, even if the **ip cef distributed** global configuration command is configured on the router.
  2. Because dCEF is not running, it is not possible to ping other routers that are directly connected to the dual RSP8.
  3. The line protocol of the CT3 interface flaps.

  Conditions: These symptoms are observed on a dual RSP8 with a CT3 interface that is configured for Stateful Switchover (SSO) and Nonstop Forwarding (NSF).

  Workaround: There is no workaround.

- CSCec44356

  Symptoms: In Layer 2 Tunneling Protocol version 3 (L2TPv3) hairpinning (local switching) configurations, matching the 802.1P values in an inbound class map does not function correctly.

Conditions: This symptom is observed on a Cisco 10720 Internet router that is running Cisco IOS Release 12.0(25) S or later releases, and only occurs when the L2TPv3 configuration uses hairpinning.

Workaround: There is no workaround.

- CSCec45704

  Symptoms: ATM binding is not used by the Tag Forwarding Information Base (TFIB) Cisco Express Forwarding (CEF) table for some prefixes of remote provider edge (PE) routers on a PE router.

  Conditions: This symptom is observed on a Cisco Route Processor Module (RPM-PR) in a cell-based Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

  Workaround: Enter the **clear ip route** *network* EXEC command.

- CSCec48025

  Symptoms: A port may go down when a channel is disabled and then reenabled while traffic passes through the port. The port failure can affect any channel and may cause some packets to be dropped for the affected channel. Packets that are smaller than an arbitrary size are dropped, and packets that are larger than this arbitrary size are unaffected.

  Conditions: This symptom is observed on the CH-E1T1 line card of a Cisco 10000 series. The **shutdown** command in both the controller and interface modes as well as explicit channel deconfiguration while traffic is passed through the channels being disabled may cause this symptom.

  Workaround: There is no workaround.

- CSCec48925

  Symptoms: When running in non-redundant PRE mode, after a crash, the line cards do not get reset. In rare cases, after Cisco IOS software reloads, there may be a mismatch between the Cisco IOS software and the line card so that the line card does not pass traffic.

  Conditions: These symptoms have been observed after Cisco IOS is restarted after a crash when running in non-redundant PRE mode. Anything that goes through the formal reload path (with a single PRE1 in the system) will properly reset the line cards on the way down. This fix resets the cards on the way up as well in case they weren't reset on the way down.

  Workaround: There is no workaround. However, after a Cisco IOS software crash, if a line card is not passing traffic, resetting the line card might fix the issue. A reload of the chassis will definitely fix the issue.

- CSCec50541

  Symptoms: A router may terminate a Secure Shell (SSH) session after the router has fallen back to local authentication and authorization. The output of a debug command may show that the router ended the session normally, as if the SSH had typed "exit" in the SSH client application.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2 or 12.3 when authentication and authorization is configured to be performed by a TACACS+ server with local fallback to the router and when the TACACS+ server goes offline. The SSH user must have been authenticated successfully at least once by the TACACS+ server.

  Workaround: Use a Telnet connection to access the router.

- CSCec56047

  Symptoms: When you configure and deconfigure Multiprotocol Label Switching (MPLS) traffic engineering (TE), stale router ID information may be used in the node structure, causing the path lookup process in the TE label switched path (LSP) topology database to fail.

Conditions: This symptom is observed when node structures are created and recycled in the TE LSP topology database without proper reinitialization of the router ID.

Workaround: There is no workaround.

- CSCec59882

  Symptoms: A Reverse Path Forwarding (RPF) check should be disabled for bootp packets with the source IP address 0.0.0.0 and the destination IP address 255.255.255.255. However, PXF currently disables RPF checks for all packets with the source IP address 0.0.0.0.

  Conditions: These symptoms have been observed on Cisco IOS Release 12.0(22)S and later.

  Workaround: There is no workaround.

- CSCec61001

  Symptoms: Parallel Express Forwarding (PXF) may stop.

  Conditions: This symptom is observed on a Cisco 10720 router that is running Cisco IOS Release 12.0(26)S and that has traffic engineering (TE) Fast Reroute (FRR) link protection when traffic flows through Ethernet over Multiprotocol Label Switching (EoMPLS) virtual circuits (VCs).

  Workaround: There is no workaround.

- CSCec61738

  Symptoms: A Cisco 7500 that is functions as a provider edge (PE) router may fail to receive an Internet Control Message Protocol (ICMP) echo message on a Multilink PPP (MLP) ingress interface.

  Conditions: This symptom is observed on a Cisco 7500 series when Virtual Private Network (VPN) routing/forwarding (VRF) is configured on the MLP interface.

  Workaround: There is no workaround.

- CSCec62568

  Symptoms: Packets with sizes that are greater than the maximum transmission unit (MTU) may be randomly dropped at the provider edge (PE) router.

  Conditions: This symptom is observed on a Cisco PE router that is configured for Layer 2 Tunneling Protocol version 3 (L2TPv3) xconnects when the **ip dfbit set** pseudowire class configuration command and the **ip pmtu** pseudowire class configuration command are set in a pseudowire class that is used for the xconnect.

  Workaround: Configure an MTU that is less than the network MTU on the CE router.

- CSCec63011

  Symptoms: A router may reload because of an NVRAM corruption.

  Conditions: This symptom is observed when NVRAM is accessed simultaneously by two processes, when one the processes has a file open, and when the second process attempts to open a nonexistent file. The error handling for the second process clears the global NVRAM pointer that is used by the first process. This situation is more likely to occur in a configuration with redundant Route Processors (RPs) but may also occur in a configuration with a single RP when two terminal windows are open.

  Workaround: There is no workaround.

- CSCec63271

  Symptoms: Some channelized PA-MC-2T3+ interfaces on a Cisco 7500 series router may go into a down/down state. When this symptom occurs, one or more groups of four T1 interfaces may go down simultaneously because of an Rx Alarm Indication Signal (AIS) alarm, and all of the interfaces associated with the down/down T1 interfaces may also go into the down/down state.

  Conditions: This symptom is observed only on a PA-MC-2T3+ port adapter. This symptom may be caused by a router or Versatile Interface Processor (VIP) reload or a circuit failure on the T3 port adapter. This symptom has not been observed on the PA-MC-T3 port adapter.

  Workaround: Perform an online insertion and removal (OIR) of the VIP that seats the PA-MC-2T3+. Make sure that you follow the guidelines for performing an OIR procedure on a Cisco 7500 series router.

  Alternate Workaround: Identify the router with four ports in the down/down state, and reload this router. You can identify the router with the interfaces in the down/down state by checking for the presence of AIS on all four ports. T1 interfaces will go down in the following combinations: 1-4, 5-8, 9-12, 13-16, 17-20, and 21-24. If T1 interfaces go down in 3-6 or 10-13 combinations, this symptom is not the reason that the interfaces are in the down/down state.

- CSCec63382

  Symptoms: When an Ethernet over Multiprotocol Label Switching (EoMPLS) virtual circuit (VC) is configured on a 3-port Gigabit Ethernet (GE) line card, the EoMPLS VC status may be in the “up” state, but no traffic passes through the EoMPLS VC.

  Conditions: This symptom is observed under rare conditions when there is some network instability (for example, when the core interface flaps).

  Workaround: One of the following workarounds may be used:

  - Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the edge-facing interface that performs EoMPLS imposition.
  - Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the core-facing interface. To identify the core-facing interface, review the output of the **show mpls l2transport vc detail** EXEC command. It will display the output interface (the core-facing interface) that is being used on a per-VC basis.
  - Reload the 3-port GE line card.

- CSCec63743

  Symptoms: Virtual circuits (VCs) go down when a policy map is attached. The policy map includes an input policy map (for example, created by entering the **set mpls experimental imposition** QoS policy-map class configuration command) and an output policy map (for example, created by entering the **queue-limit** policy-map class configuration command).

  Conditions: This symptom is observed on a Cisco router with an Engine 2 (E2) 8xOC3 ATM line card and an Engine 3 (E3) 4xOC12 ATM line card.

  Workaround: Reload the router.

- CSCec64570

  Symptoms: The node of a local Label Switch Controller (LSC) that is part of a Multiprotocol Label Switching (MPLS) cell-based network may observe the following symptoms:

  - The local provider edge (PE) router cannot ping the remote customer edge (CE) router.
  - The remote PE router cannot ping the local CE router.
  - The local PE router can ping the remote CE router with type of service (Tos) equal to 0xe0.

  - The remote PE router can ping the local CE router with ToS equal to 0xe0.
  - A ping with the route record option does not work in either direction.
  - A ping with the trace route option does work.

  Conditions: These symptoms are observed on the LSC of a Cisco MGX Route Processor Module (MGX-PRM-PR-512) that is running Cisco IOS Release 12.2(15) T4a.

  Workaround: From the node of the local LSC that is observing the symptoms, enter the **clear ip route** *network* EXEC command.

- CSCec65940

  Symptoms: Packets that go to destinations learned by Border Gateway Protocol (BGP) may be dropped for up to 60 seconds or so as soon as the routes are installed. The packet loss occurs only for the first minute or so after the BGP session comes up. After that time period, packet forwarding functions correctly.

  Conditions: This symptom is observed when all of the following conditions occur:

  - The BGP session involves a Multiprotocol Label Switching (MPLS) label exchange (external BGP [eBGP] single-hop sessions are most likely to be affected).
  - The BGP peer is reachable via a link with PPP encapsulation.
  - The router in question is running Cisco IOS Release 12.0(22)S or a later release.

  Workaround: Since the symptom is specific to PPP encapsulation, one way to avoid the symptom is to use another form of encapsulation (for example, High-Level Data Link Control [HDLC]).

- CSCec66970

  Symptoms: A Section Data Communications Channel (SDCC) interface on a channelized IP Services Engine (ISE) OC48 line card no longer functions.

  Conditions: This symptom is observed in Cisco IOS software releases that are after Release 12.0(26)S.

  Workaround: There is no workaround.

- CSCec67272

  Symptoms: When you reload a Multiprotocol Label Switching (MPLS) provider edge (PE) router that has 20 PA-MC-2T3+ controllers and 780 channelized interfaces, the first PA-MC-2T3+ controller may have many channelized interfaces in the down/down state.

  Conditions: This symptom is observed on an MPLS PE router that has the channelized interfaces that are in the down/down state directly connected to a customer edge (CE) router. If the connection is a T1 interface, then the interfaces on the CE router are in an up/down state. If the connection is sub-T1 (fractional T1), then the interfaces on the CE router are in an up/up state.

  Workaround: Reload only the CE router and all the interfaces will go to the up/up state on both the CE router and the PE router.

- CSCec67980

  Symptoms: The standby Route Processor may reload shortly after if boots up if the **snmp-server packetsize** *byte-count* global configuration command is included in the configuration.

  Conditions: This symptom is observed on a standby RP if the packet size of the Simple Network Management Protocol (SNMP) server is included in the configuration of the router.

  Workaround: Do not specify the packet size of the SNMP server in the configuration of the router.

- CSCec68831

  Symptoms: When a router boots up with an existing policy map, the quality of service (QoS) marking function may not function correctly depending upon the combination of line cards that are in the router. The symptom is observed more often with channelized port adapters.

  Conditions: This symptom has been observed on a Cisco 7500 series router with many channelized port adapter when the policy is applied to the input direction of the interface.

  Workaround: After the router boots up, recreate the new policy map and apply it to the input direction of the channelized interface.

- CSCec69392

  Symptoms: The Forwarding Information Base (FIB) may be disabled on various types of line cards.

  Conditions: This symptom is observed on a Cisco 12000 series after you have performed an online insertion and removal (OIR) of the clock scheduler card (CSC).

  Workaround: There is no workaround.

- CSCec69756

  Symptoms: You may not be able to configure the maximum transmission unit (MTU) on a virtual template.

  Conditions: This symptom is platform independent.

  Workaround: There is no workaround.

- CSCec69982

  Symptoms: You may not be able to reestablish a direct label distribution protocol (LDP) session over an Any transport over MPLS (AToM) virtual circuit (VC).

  Conditions: This symptom is observed on a Cisco router when the **mpls ip** interface configuration command is not enabled on any interface and when you delete and reenter the **xconnect** ATM VC configuration command in quick succession.

  Workaround: Remove the AToM VC, delete and reenter the **xconnect** interface configuration command, wait until the router returns to the prompt, and recreate the AToM VC.

- CSCec70301

  Symptoms: The output queue of an 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) may be stuck, even though the controller is up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0 S, Release 12.1 E, or Release 12.2 S after you have performed an online insertion and removal (OIR) of the PA-MC-8TE1+.

  Workaround: Reload the router.

- CSCec73093

  Symptoms: NetFlow export may not function when a service policy is enabled.

  Conditions: This symptom is observed on a Fast Ethernet interface that has 802.1q encapsulation enabled.

  Workaround: There is no workaround.

- CSCec75189

  Symptoms: Two interfaces may have the same Cisco Express Forwarding (CEF) interface description block (IDB) when the following configuration sequence occurs:

  – Create subinterface.

  - Delete subinterface.
  - Create another subinterface.
  - Create the first subinterface again.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0 S or Release 12.2 S.

  Workaround: There is no workaround. Reload to clear the condition.

- CSCec76078

  Symptoms: A 4-port OC-3 ATM line card may reload within a few minutes.

  Conditions: This symptom is observed on a 4-port OC-3 ATM line card with several ports connected but without the Tx clocks being synchronized on the ports.

  Workaround: Synchronize all Tx clocks, or disconnect the ports.

- CSCec77576

  Symptoms: The following error messages may be displayed on a Cisco router when the **show ip cef inconsistency now** EXEC command is entered:

  ```
  Error: Time-out waiting for linecards ( 0 1 2 3 4 9 ) to respond.
  Error: Failed to run full-scan-rp checker
  ```

  The (0 1 2 3 4 9) listing in the error message refers to the populated slots in the router.

  Conditions: This symptom is observed on a Cisco 7500 series router after a Stateful Switchover (SSO) has occurred.

  Workaround: There is no workaround.

- CSCec77699

  Symptoms: In a Fast Software Upgrade (FSU) and software downgrade test environment, a standby Performance Routing Engine (PRE) may reload.

  Conditions: This symptom is observed on a Cisco router when an FSU downgrade from Cisco IOS Release 12.0(26)S to Release 12.0(23)S4 or Release 12.0(24)S3 occurs.

  Workaround: Reboot the router.

- CSCec80049

  Symptoms: When a tunnel interface goes down, a new Label Switched Path (LSP) is not signaled until the forwarding adjacency hold timer expires.

  Conditions: This symptom is observed on a Cisco router that is configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

  Workaround: There is no workaround.

- CSCec86963

  Symptoms: A Versatile Interface Processor (VIP) may reload and cause the Route Switch Processor (RSP) to reload after an input set policy is added to a Frame Relay (FR) map class.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: Use traffic policing to set the input policy.

- CSCec87815

  Symptoms: A buffer leak may occur in the Multilink PPP (MLP) header pool on a Versatile Interface Processor (VIP). The speed of the leak depends on the rate of traffic that is flowing between the interface of the VIP and the interface on the other end. The leak may eventually cause memory allocation failures (MALLOCFAIL) on the VIP and may result in memory fragmentation.

  Conditions: This symptom is observed on a Cisco 7500 series when all of the following conditions are present:

  - Distributed Cisco Express Forwarding (dCEF) is enabled.
  - An MLP bundle that includes interfaces on the VIP is configured.
  - A different interface on the same VIP performs some type of fancy queueing such as committed access rate (CAR), policing, or Class-Based Weighted Fair Queueing (CBWFQ).
  - Packets are locally switched between the MLP interface and the interface that is configured for fancy queueing.

  Workaround: Stop the leak by removing the fancy queueing from the VIP interface.

  Alternate Workaround: Move the MLP interfaces to a different VIP that does not have an interface that performs fancy queueing.

- CSCec87862

  Symptoms: A Cisco router may experience a Parallel Express Forwarding (PXF) reload, and the following error messages may appear in the log:

  ```
  %TOASTER-2-FAULT: T0 Local Bus Exception: CPU[t0r2c2] CM at 0x0A00 LR 0x0A6
  %TOASTER-2-FAULT: T0 Exception summary: CPU[t0r2c2] Stat=0x00000022 HW=0x00000000
  LB=0x00000040 SW=0x00000000
  ```

  Conditions: This symptom is observed on a Cisco 10720 router that is running the c-10700-p-m image of Cisco IOS Release 12.0(24)S3.

  Workaround: There is no workaround.

- CSCec89886

  Symptoms: Traffic that flows on the first path or access unit (AU) controller (on each physical port) of a 4-port channelized OC3 STM-1 line card may stop after a Performance Routing Engine (PRE) cutover. Other paths or AUs may not be affected.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCed00798

  Symptoms: Packets may be dropped at the output interface on a Cisco router.

  Conditions: This symptom is observed on a Cisco 10720 router when there is PPP encapsulation on the incoming interface and the packets have Multiprotocol Label Switching (MPLS) labels.

  Workaround: Disable PPP encapsulation, and use High-Level Data Link Control (HDLC) for the incoming interface.

- CSCed01648

  Symptoms: When an interface is shut down and the router reloads, the **shutdown** interface configuration command disappears from the running configuratio**n** and the interface becomes active again. However, the **shutdown** command is still in the startup configuration.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Shut down the interface each time after the router reloads.

- CSCed03356

  Symptoms: The deletion of an ATM subinterface may occasionally cause a secondary Performance Routing Engine (PRE) to reload.

  Conditions: This symptom is observed on a Cisco 10000 series that has two PREs that are configured for high availability.

  Workaround: There is no workaround. However, the symptom does not affect performance. The primary PRE continues to forward traffic. The secondary PRE will reload if it is configured to do so.

- CSCed27956

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed38527

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

- CSCed46936

  Symptoms: If the **service-policy** {**output**} command is configured on a PA-MC-8E1/120 interface, the ping of a neighbor router fails. Other IP traffic also stops. When this command is removed, the ping and other IP traffic starts passing through this line.

  Conditions: This symptom occurs when the **service-polic**y {**output**} command is configured on a Cisco 7200 series router on a channelized interface, such as the PA-MC-8E1/120 interface.

  Workaround: Remove the **service-policy** {**output**} command.

- CSCed50514

  Symptoms: A Cisco router reloads with unexpected exception and tracebacks.

  Conditions: If you have a serial interface configured, and you try to remove the AUG controller, the router reloads. See the following example:

```
router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#cont sonet 3/0/0
router(config-controller)#no aug cont
router(config-controller)#no aug controller
router(config-controller)#
```

  Workaround: There is no workaround.

- CSCed54342

  Symptoms: A reload occurs that sends a Cisco 10000 series router into ROMMON state.

  Conditions: This symptom occurs after configuring CHOC3 interfaces and then performing the **shut** command followed by the **no shut** command. The reload sends the Cisco 10000 series router into ROMMON state.

  Workaround: There is no workaround.

- CSCin35896

  Symptoms: The outgoing label for a prefix that is received through Border Gateway Protocol (BGP) IP version 4+ (IPv4+) labels may not be installed in the Tag Forwarding Information Base (TFIB).

  Conditions: This symptom is observed if the router that performs a BGP IPv4+ label exchange receives a label withdraw request for an MPLS label from a BGP peer that is followed by a readvertisement of the label. This symptom occurs if the **no mpls ip** global configuration command followed by the **mpls ip** global configuration command is executed on the peer router; however, the label withdraw request may be triggered in other ways also.

  Workaround: Enter the **clear ip route** *prefix* EXEC command to correct the symptom.

- CSCin48418

  Symptoms: A Cisco router may reload when you enter the **show running-config** privileged EXEC command.

  Conditions: This symptom is observed when you configure one virtual circuit (VC) more than the maximum number of allowed connections.

  Workaround: Do not configure more connections than the maximum number of allowed connections.

- CSCin49458

  Symptoms: Pings between two customer edge (CE) routers may fail.

  Conditions: This symptom is observed after a high traffic load has occurred for a short period of time on Any Transport over Multiprotocol Label Switching (AToM) Layer 2 Tunneling Protocol version 3 (L2TPv3) virtual circuits (VCs). The VCs stay up, but pings may fail.

  Workaround: Reload the microcode onto the line card on which the VCs are configured.

- CSCin49862

  Symptoms: When the Any Transport over MPLS (AToM): ATM Cell Relay over MPLS feature is configured in virtual circuit (VC) mode or virtual path (VP) mode, not all AToM VCs or VPs may become established, and the output of the **debug xconnect error** privileged EXEC command may display the following message:

  XC AUTH [<ipaddr>, <vcid>]: Mismatch MTU

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with a large number of ATM over Multiprotocol Label Switching (ATMoMPLS) cell mode circuits (more than 1000 ATM VCs or VPs) when interfaces flap, causing all VCs or VPs to attempt to reestablish themselves simultaneously.

  Workaround: Deconfigure the Any Transport over MPLS (AToM): ATM Cell Relay over MPLS feature from the affected VC or VP; then, reconfigure the feature on the VC or VP.

- CSCin50883

  This caveat consists of four symptoms, four conditions, and a single workaround for all four symptoms and conditions:

  Symptom 1: A “PCMCIA-DIBERR” error message may be displayed.

  Condition 1: This symptom is observed when you enter the **show** *flash-filesystem***:** EXEC command for a Personal Computer Memory Card International Association (PCMCIA) disk that is formatted for low-end file system (LEFS).

  Symptom 2: An “Invalid DOS Media” error message may be displayed.

  Condition 2: This symptom is observed when you remove a compact Flash card that is formatted for MS-DOS FS, you replace it with one that is formatted for LEFS, and you enter the **show:** *flash-filesystem***:** EXEC command.

  Symptom 3: A compact Flash card that is configured for LEFS may not be recognized.

  Condition 3: This symptom is observed when you perform an online insertion and removal (OIR) and you replace an Advanced Technology Attachment (ATA) Flash card with a compact Flash card that is configured for LEFS.

  Symptom 4: A traceback for a duplicate file system may be generated in the file system table.

  Condition 4: This symptom is observed when you perform an OIR and you replace a compact Flash card that is configured for LEFS with an ATA Flash card.

  Workaround for all four symptoms and conditions: Before you enter any command or perform an OIR, enter the **show version** EXEC command. Doing so forces the PCMCIA card or the compact Flash card to be reread and clears the difficulties.

- CSCin51588

  Symptoms: When you reload the microcode onto an enhanced 8-port multichannel T1/E1 port adapter (PA-MC-8TE1+) while traffic is flowing through the port adapter, the following error message may appear:

  ```
  %RSP-3-RESTART: interface Serial0/0/4:0, not transmitting
  ```

  In most cases, the interfaces of the port adapter recover on their own. In very rare cases, the execution of a Cbus Complex occurs.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: If the interfaces of the port adapter do not recover on their own, execute a Cbus Complex.

- CSCin52105

  Symptoms: A Multilink Frame Relay (MLFR) bundle interface may flap along with its member links.

  Conditions: This symptom is observed when distributed MLFR is configured on a nonchannelized port adaptor such as a 4-port serial enhanced port adapter (PA-4T+) or an 8-port serial port adapter (PA-8T).

  Workaround: There is no workaround.

- CSCin52927

  Symptoms: A Cisco 7200 series may reload after you change the maximum transmission unit (MTU) of an Inverse Multiplexing over ATM (IMA) interface while traffic is flowing.

  Conditions: This symptom is observed when the Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: VC Mode feature is configured on the IMA interface.

  Workaround: There is no workaround.

- CSCin53040

  Symptoms: A secondary Route Switch Processor (RSP) that is configured with 512 MB RAM may not recognize the 512 MB RAM.

  Conditions: This symptom is observed on a Cisco 7500 series that has a primary and a secondary RSP and that runs a Cisco IOS image that has a size larger than 20 MB.

  Workaround: Configure the secondary RSP with 256 MB RAM.

- CSCin53682

  Symptoms: A provider edge (PE) router may reload when packets are forwarded while a remote Virtual Private Network (VPN) prefix is being reresolved.

  Conditions: This symptom is observed when the MPLS VPN-Inter-AS-IPv4 BGP Label Distribution feature is configured for option 4, that is, for a non-VPN transit provider and a multi-hop external Border Gateway Protocol (eBGP) connection between route reflectors (RRs).

  Workaround: For the exchange of PE loopback addresses between autonomous systems, do not use eBGP with IPv4 label distribution. Rather, configure redistribution into Interior Gateway Protocol (IGP) or static routes.

- CSCin57432

  Symptoms: A Versatile Interface Processor (VIP) may run low on memory when a high rate of traffic is sent across the Multilink Frame Relay (MFR) interface.

  Conditions: This symptom is observed when an MFR interface is distributed onto a line card.

  Workaround: There is no workaround.

- CSCin57433

  Symptoms: All of the configured data-link connection identifiers (DLCIs) on a Multilink Frame Relay (MFR) interface are not active.

  Conditions: This symptom is observed if a Cisco router is booted with MFR in the startup configuration.

  Workaround: There is no workaround.

- CSCin57765

  Symptoms: A router may become unresponsive and may reload when you append a file whose size is not a multiple of 512 bytes to an Advanced Technology Attachment (ATA) Flash card (for example, bootdisk, disk0, disk1).

  For example, this situation may occur when you enter the **show** *command* **| tee /append** *url* privileged EXEC command.

  Conditions: This symptom is observed on a Cisco platform that runs a Cisco IOS image that contains the fix for caveat CSCdz27200 and that utilizes an ATA Flash card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz27200. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: Write the output of the **show** command to a new file instead of appending it to an existing file by entering the **show** *command* **| tee** *url* privileged EXEC command.

- CSCuk39887

  Symptoms: Traffic that passes through a tunnel interface may be dropped because the application inspection (also referred to as "fixup") is disabled on the tunnel interface adjacency.

  Conditions: This symptom is observed in Cisco IOS Release 12.0(24)S or a later release.

  Workaround: Toggle Cisco Express Forwarding (CEF) by entering the **no ip cef distributed** global configuration command followed by the **ip cef distributed** global configuration command.

- CSCuk43457

  Symptoms: The output of the **show route-map** EXEC command may indicate that duplicate traffic indices have been configured.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured for Border Gateway Protocol (BGP) policy accounting. The symptom may also occur on other platforms.

  Workaround: There is no workaround.

- CSCuk44928

  Symptoms: When you save a configuration first to the standby Performance Routing Engine (PRE) and then to the active PRE, the configuration may not be saved and the following error message may be generated:

  ```
  startup-config file open failed (Device or resource busy)
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with redundant PREs and that runs Cisco IOS Release 12.0(26)S. The symptom may also occur in other Cisco IOS releases.

  Workaround: There is no workaround.

- CSCuk46911

  Symptoms: When you enter the **exec slot 0 clear log** EXEC command on a Cisco 12000 series router, the line card may stall.

Conditions: This symptom is observed on a Cisco 12000 series that is running Cisco IOS Release 12.0 S.

Workaround: Enter the **clear log** EXEC command directly on the line card.

- CSCuk47444

  Symptoms: Memory allocated by the **ip cef linecard ipc memory** *kbps* global configuration command is not freed when a standby Route Processor (RP) becomes an active RP.

  Conditions: This symptom is observed only when the **ip cef linecard ipc memory** *kbps* global configuration command is used because the allocated memory on the standby RP memory is not freed when the standby RP switches over to become the active RP.

  Workaround: There is no workaround.

- CSCuk47482

  Symptoms: A router may reload unexpectedly while you disable label distribution protocol (LDP) on an interface.

  Conditions: This symptom is observed on a router that has several interfaces that are configured for LDP when you disable LDP on all interfaces and when there is still one open TCP connection that is passively used by LDP while you disable LDP on the last interface.

  Workaround: There is no workaround.

- CSCuk47528

  Symptoms: Packet redirection to a cache may not occur even though Web Cache Communication Protocol (WCCP) is enabled and the cache farm has formed successfully. The symptom may be invisible to end users because packets, usually packets that are part of HTTP sessions, still flow successfully to and from their original destinations.

  Conditions: This symptom is observed on a Cisco platform when both WCCP and Cisco Express Forwarding (CEF) are enabled.

  Workaround: Disable CEF on all interfaces on which a WCCP redirect statement is configured.

- CSCuk48314

  Symptoms: During an SSO switchover, the newly active Route Processor (RP) may output the following error message:

  ```
  %SCHED-7-WATCH: Attempt to monitor uninitialized watched queue (address 0).
  -Process= "CEF LC IPC Background"
  ```

  This error is harmless, and no functional problem will occur when this error is received.

  Conditions: This symptom occurs during an SSO switchover.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCeb07106

  Symptoms: The following error message appears in the log of a Cisco router:

  ```
  %TCP-6-TOOBIG: Tty0, too many bytes of options (44)
  ```

  Conditions: This symptom is observed when numerous TCP options are configured on the router.

  Workaround: Reduce the number of TCP options used (for example, selective-ack, timestamps, or BGP md5-password).

Wide-Area Networking

- CSCdx72556

  Symptoms Link-control-protocol (LCP) negotiations may fail, and a “failed to negotiate with peer” message may be displayed.

  Conditions This symptom is observed on a Cisco universal access server if the peer sends more than five Configure-Negative acknowledgments (CONFNAKs) or Configure-Rejects (CONFREJs) on the link for the current or previous LCP negotiation.

  Workaround Configure the **ppp max-failure 10** command on the link to allow the remote peer to exhaust the Negative acknowledgment (NAK) or Reject acknowledgment (REJ) count and resume negotiations before the Cisco universal access server drops the link.

- CSCeb33417

  Symptoms: A router may reload when it tries to add a permanent virtual circuit (PVC) to a bundle link.

  Conditions: This symptom is observed when a normal Local Management Interface (LMI) frame is received without the User-Network Interface (UNI) fragmentation header. This causes the frame to be processed on the bundle link instead of on the bundle.

  Workaround: There is no workaround.

- CSCec08632

  Symptoms: If a ping to the tunnel end of an L2TP network server (LNS) fails, a large number of packets are continuously generated, and the router may reload with a memory allocation failure error message.

  Conditions: This symptom is observed on a Cisco router that is configured for voluntary Layer 2 Tunneling Protocol (L2TP) or client-initiated L2TP tunneling.

  Workaround: There is no workaround.

- CSCec13050

  Symptoms: A router may reload when you enter the **show running-config** privileged EXEC command after a channel group interface is created on the router.

  Conditions: This symptom is observed if you create the channel group interface, configure Frame Relay (FR) encapsulation on the interface, and then delete the interface without first removing the FR encapsulation.

  Workaround: Remove the FR encapsulation before deleting the channel group interface.

- CSCin51321

  Symptoms: Traffic that is switched via Frame Relay may not pass through a 2-port multichannel T3 port adapter (PA-MC-2T3+) in unchannelized mode.

Conditions: This symptom is observed on a Cisco 7500 series that is configured for distributed switching.

Workaround: Disable distributed switching.

- CSCin53115

  Symptoms: It may not be possible to add a bundle link to a Multilink Frame Relay (MFR) interface.

  Conditions: This symptom is observed on a Cisco router that has data-link connection identifier (DLCI) 896 configured.

  Workaround: Do not configure DLCI 896.